S. HRG. 105–894

SMALL BUSINESSES TO GLOBAL CORPORATIONS: WILL THEY SURVIVE THE YEAR 2000?

HEARING

BEFORE THE

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

ON

THE EFFECT OF Y2K ON GENERAL BUSINESS—A TERM THE ENCOMPASSES THE SPECTRUM OF AMERICAN COMMERCE RANGING FROM OVER 5 MILLION SMALL FIRMS AT ONE END OF THE SPECTRUM TO GLOBAL CORPORATIONS AT THE OTHER END

OCTOBER 7, 1998

Printed for the use of the Committee

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE
51-564 CC WASHINGTON : 1999

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

SPECIAL COMMITTEE ON THE
YEAR 2000 TECHNOLOGY PROBLEM

[Created by S. Res. 208, 105th Cong., 2d Sess. (1998)]

ROBERT F. BENNETT, Utah, *Chairman*

JON KYL, Arizona
GORDON SMITH, Oregon
SUSAN M. COLLINS, Maine
TED STEVENS, Alaska, *Ex Officio*

CHRISTOPHER J. DODD, Connecticut, *Vice Chairman*
JEFF BINGAMAN, New Mexico
DANIEL PATRICK MOYNIHAN, New York
ROBERT C. BYRD, West Virginia, *Ex Officio*

Robert Cresanti, *Staff Director*
T.M. (Wilke) Green, *Minority Staff Director*

CONTENTS

OPENING STATEMENT BY COMMITTEE MEMBERS

CHRONOLOGICAL ORDER OF WITNESSES

APPENDIX

Alphabetical Listing and Material Submitted

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Note: Responses to questions submitted by Chairman Bennett to Mr. Lou Marcoccio were not received at the time the hearing was published.

SMALL BUSINESSES TO GLOBAL CORPORATIONS: WILL THEY SURVIVE THE YEAR 2000?

WEDNESDAY, OCTOBER 7, 1998

U.S. SENATE,
SPECIAL COMMITTEE ON THE YEAR 2000
TECHNOLOGY PROBLEM,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Robert F. Bennett (chairman of the committee), presiding.

Present: Senators Bennett, Smith, and Collins.

OPENING STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM UTAH, CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Chairman BENNETT. The committee will come to order. I have just received word that we have two stacked roll call votes scheduled starting at 10 o'clock. I have said before, somewhat facetiously, the Senate gets in the way of the work of the Senate from time to time. We apologize in advance to our witnesses for the disruption that might come as senators will have to leave to go to the floor to cast these votes; we are very grateful to all of the witnesses for their coming and being with us today at this hearing on the general business sector.

This is the committee's ninth and final hearing this year, and in every one of our hearings we have strived to increase awareness and disseminate reliable preparedness information as well as facilitate solutions. I believe we have done that. In spite of the efforts of the committee, however, recent polls say that only 30 percent of Americans have even heard of the Year 2000 problem and that is a little disquieting. There are now 450 days between us and the new century so that the work of this committee and everyone connected with this problem becomes more urgent with each passing day.

Now we have gone through the top priorities that the committee laid out at the outset starting with the power grid going through telecommunications and so on. So we come to general business activity and just because it comes after some of these other vital infrastructure priorities does not mean that it cannot have a major impact on what happens in the Year 2000. "General business" is the term that encompasses the spectrum of American commerce from over 5 million small firms at one end to global corporations at the other end. Every one of these companies in one way or another faces a Year 2000 challenge—from the PC on which you keep your books all the way up through the systems that automate offices, credit card point of sale systems, and just in time inventory systems.

One of today's witnesses will warn us that over 700,000 small firms are at risk of closing their doors or being severely crippled by Year 2000 problems. So the awareness challenge that we have taken on this committee is still very necessary. Now global corporations face complex problems because of their dependence on thousands of suppliers, distributors, and frankly customers; a customer can have a problem that can kick back into your corporation in a variety of ways. These problems are both domestic and international. Businesses must be concerned not only about Y2K readiness of their partners but the infrastructure of the companies in which they reside. Perhaps in next year's hearings I will focus more on international problems and move in that direction.

Today, the Gartner Group is releasing some alarming new research data which shows that 66 percent of the companies in critical industries such as health care and food processing will likely experience at least one mission critical systems failure. In addition, 50 percent of the companies in critical trading partner countries such as Germany, Japan, Saudi Arabia, and Venezuela will experience similar failures, and if these predictions are correct and nothing is done in the 450 days remaining, Y2K could deliver a devastating blow to an already troubled global economy.

If I sound overly serious, it is not because I am grabbing for the headlines but because I am hoping to reach people who are currently unaware of where they are. It reminds me of a paraphrase from the poem by Rudyard Kipling: If you can keep your head when all around you are losing theirs, you do not understand the situation. [Laughter.]

[The prepared statement of Chairman Bennett can be found in the appendix:]

Chairman BENNETT. Now, before we hear from our witnesses I would like to recognize Senator Collins for any opening statement that she might have. I would also comment that her colleague Senator Olympia Snowe, who has been part of this effort even though she is not a member of this committee, has a statement that she would like included in this record. She has held a number of hearings around the State of Maine on small business issues and so it is appropriate that her contribution to the committee would be included.

[The prepared statement of Senator Snowe can be found in the appendix.:]

Chairman BENNETT. Senator Collins.

OPENING STATEMENT OF HON. SUSAN M. COLLINS, A U.S. SENATOR FROM MAINE

Senator COLLINS. Thank you very much, Mr. Chairman. I want to first thank you for your continued leadership on this critical issue. Over the past 4 months, this committee has examined vital areas of our country's technological infrastructure. We started in June with our utilities hearing, and since that time the committee has focused on telecommunications, banking and finance, transportation, and most recently emergency preparedness. But of all the hearings that we have held, today's hearing with its focus on Y2K's impact on business, especially the impact on small business, might well be our most important endeavor to date.

Our Nation's 23 million small businesses create 2 out of every 3 new jobs, represent over 90 percent of all employers, and are responsible for more than half of our nation's technological innovation. In my home State of Maine, they are truly the backbone of our economy. While we have received assurances of other industry sectors' preparedness for Y2K, there is considerable concern about the small business sector. Many small businesses are having difficulty in determining how they will be affected by Y2K and what they should do about it. Many of them face not only technological but also financial challenges in becoming Y2K compliant. Most of all, they simply need practical information about what to do.

The good news is that information resources are available for small businesses to assist them in figuring out what to do. In fact, I look forward to welcoming two people who know how to help small businesses and are working everyday to tackle the Y2K problem. First, I want to welcome Fred Hochberg, the Deputy Administrator of the SBA, an organization with which I am very familiar because I served at one point as the New England administrator of the SBA. The SBA joined Senator Snowe, as the chairman has mentioned, in Maine in August to roll out the agency's "Are You Y2K OK?" program which encourages small businesses throughout the country to identify potential Y2K problems, take action on them, and stay informed about new developments. This is an excellent outreach program and I want to commend SBA for its leadership role on Y2K.

I also am especially proud to welcome Rod Rodrigue from Maine. I had the opportunity to meet with Rod last month in my office and was impressed by the tremendous amount of knowledge and energy he brings to this issue. Thanks to his leadership, the Maine Manufacturing Extension Partnership has taken the initiative in my State in reaching out to small businesses to help them cope with the Y2K challenge.

The Maine Manufacturing Extension Partnership uses a diagnostic software tool to assist businesses in identifying specific Y2K problem areas and then provides a road map for businesses to find further information to help them with the Y2K remediation process including links to SBA loans if necessary. I believe that Congress should take a very close look at this model which is funded through the National Institute of Standards and Technology as well as the Department of Commerce.

Mr. Chairman, by their very definition, entrepreneurs are risk managers. In the years that I have been working with small businesses and based on my own family's 150 years of continuous operation as a small business, I am very aware of the countless experiences where the entrepreneurial spirit has propelled small business owners to overcome major obstacles to succeed.

While we hear about the reasons for concern about small businesses and their ability to cope with Y2K in today's hearing, we should not lose sight of their amazing and continual ability to adapt to changed circumstances. Coupled with tools and resources from organizations like the SBA and the Maine MEP, it is my expectation that small businesses will, in fact, succeed in solving the Y2K problem. I look forward to learning more from today's witnesses about how the Federal Government can assist them in meeting this goal. Thank you, Mr. Chairman.

[The prepared statement of Senator Collins can be found in the appendix.]

Chairman BENNETT. Thank you very much. We have divided up the responsibilities in the committee according to the seven priorities that we outlined and the seven members of the committee. Senator Smith, who is himself a small businessman—actually his business has grown quite large, has led the committee on this issue. [Laughter.]

During my first campaign, I was accused of being a big businessman, and I said, well, I did not start out that way. [Laughter.]

But I am not going to give it back. This particular assignment of dealing with general business Y2K problems has been given to Senator Smith and he has responded very well and we appreciate his leadership and help on this. Senator Smith.

OPENING STATEMENT OF HON. GORDON SMITH, A U.S. SENATOR FROM OREGON

Senator SMITH. Thank you, Mr. Chairman. I appreciate being able to work with you and the excellent leadership you have given in addressing this Y2K problem. I also want to thank our distinguished witnesses who are with us today for taking time to help us address the challenges facing the entire business sector at both the large and small ends of the scale.

With American business today becoming more and more dependent on technology, I hope this hearing will be a stepping stone for all small businesses to inch closer to full preparedness for the Year 2000. Those most at risk for the Y2K failures are small and medium-sized companies, not their larger counterparts. Many small companies have not yet realized the extent to which the Y2K computer problem will affect their businesses and may not have access to capital to cure such problems before the Y2K issue causes them disastrous effects.

This is why it is so important for the Federal Government to both raise awareness of the problem as well as find emerging solutions. In my former life, as the chairman mentioned, I was a food processor. I called myself a pea picker from Pendleton, OR and owned a small frozen food processing plant. I can assure you that any interruption within the farm to fork chain can result not only in direct loss to those who supply food but will likely translate into food shortages and price increases nationwide.

As with many businesses, food suppliers are increasingly dependent on computerized processing and information exchange. For example, farmers and ranchers use electronically equipped irrigation systems, animal systems and transport systems. Food processors rely on automated systems that help prepare and package consumer ready products. Distributors, wholesalers, and retailers depend on computer-driven equipment to transport, deliver, store, display, and sell food products. Inventory and accounting systems, harvesting equipment, grain elevators, refrigeration and security systems all depend on the computations of computers. Mr. Chairman, I know that there was some difficulty in getting some of our larger retailers and food processes to participate today, but I am happy to report that we will hear from a representative of one of Oregon's food companies and they have been working very hard on the Y2K issue.

I am proud to introduce Harold Schild, the president and CEO of Tillamook County Creamery, who is one of our witnesses today from Tillamook, OR. If you all have not tried Tillamook cheese and ice cream, it is the best in the world. No offense meant to any of my Wisconsin colleagues.

Chairman BENNETT. We will take you to Cash Valley. [Laughter.]

Senator SMITH. I look forward to hearing Mr. Schild's testimony to address the real problems with which typical small business is confronted and specifically the food industry in its approaches to addressing the Y2K problem. Another company from Oregon, Norpac Foods, has also been leading the effort in addressing the Y2K problem in the frozen food business. While their representative is not here today, Mr. Chairman, they have provided a statement that is very helpful and insightful, and I ask that that be included in the record.

Chairman BENNETT. Without objection.

[The prepared statement of Norpac Foods can be found in the appendix.]

Senator SMITH. I am also pleased that the Deputy Administrator of the Small Business Administration, Mr. Fred Hochberg, is here before us today. The SBA has been one of the leading Federal agencies actively raising public awareness for Year 2000, and I would like to commend the agency for its aggressive outreach programs to small business. I know my constituents in Oregon have found the SBA website a very useful and informative tool.

Mr. Hochberg, I am interested in your opinion regarding the recent legislation passed by the Senate Small Business Committee that requires SBA to establish a Y2K loan program. I understand this loan program would establish a new short-term loan program under which the SBA would guarantee up to 50 percent of the value of private sector loans up to a total loan value of $50,000 for small businesses to become Y2K compliant. So your views on that I am interested in. If you or any of the witnesses can testify on the impact this legislation will have, it will be helpful to all small business.

As we work toward addressing the Y2K problem, let us not forget that many of our international neighbors are still very far behind. We need to continue to encourage foreign countries to focus on the impacts of Y2K since it could potentially shut down an entire country. With this in mind, I look forward to hearing more specifics on Y2K challenges facing our small businesses and our global corporations and, Mr. Chairman, I thank you.

[The prepared statement of Senator Smith can be found in the appendix.]

Chairman BENNETT. Thank you very much. Now, before we get into the subject of today's hearing specifically, I would like the members of the committee to meet one of my constituents, Laurene West, who is a registered nurse from Salt Lake City, UT. Her special medical circumstances graphically demonstrate that the Y2K problem is not just a technological problem or a business problem, but can be a very personal one. This very capable and articulate woman is living proof that the Y2K problem has potential to take a very serious toll. And she has courageously agreed to share her story with us. So I would ask her to come forward and be our first witness this morning. Even though it is not specifically on the issue of small business, I think you will find it very worthwhile. Ms. West, we welcome you and again we thank you for your willingness to share what must be a very difficult personal odyssey with us, but I think the committee and those who are watching on television and elsewhere will be greatly benefitted by your willingness to do this and we are grateful to you.

STATEMENT OF LAURENE L. WEST

Ms. WEST. Thank you, Senator Bennett. Can you hear me?

Chairman BENNETT. Yes. If you could get a little closer to the microphone. These microphones are not going to be threatened by Y2K problems. [Laughter.]

They are low enough tech and old enough that they are not a problem. So if you could get it as close to you as you can, we would appreciate it.

Ms. WEST. Thank you. I appreciate the invitation to present to you my concerns and my health history. Seated before you this morning, I probably give the impression that I am good health. I am not. Without a daily supply of medication and a coordinated community effort on the part of the health care community, I will be a casualty of the Year 2000; I will die.

I had a tumor removed from the center of my brain, and I now require daily medication to prevent the tumor from returning. Additionally, when I had the first of 13 surgeries on my head, I acquired a staph infection which now requires—the infection that I have in my head is not sensitive to any known oral antibiotic. Therefore, I am dependent on a continual supply of IV antibiotics. I am a registered nurse. For 20 years I worked in critical care settings of acute care facilities, and for the last 14 years I have worked with developing and implementing medical information systems. I share that with you so that you know or that you understand that I know health care. I know it from being a clinician. I know health care also from being a recipient of care and I know how the Year 2000 will affect health care.

My message today is twofold. First as a clinician, we have all heard the media reports about what the Year 2000 will do to the power grid, national security, air traffic. All hospitals are at risk if we do not have power, but I can bring an army of clinicians into any facility and keep patients alive basically by doing CPR, but I cannot keep patients alive if I do not have a continual supply of their medications.

My second message is that all Americans will be affected by a disruption in the supply and distribution of medications, particularly those of us who are alive only because on a daily basis, I take drugs to keep my tumor from growing and to keep the infection in my head from spreading. And what I find amazing is that my medication requirements are minimal compared to those of diabetics, transplant patients, patients with implantable devices, patients who have hypertension, who have cardiac difficulties. Those people have no time if they do not have access to their medications.

We need to begin immediately to create a public awareness program. We need to teach the people of our country what they can do to prepare. AARP needs to know. They need to talk to their membership and let those people know that they are going to have a store of their medications. They need to stockpile their medications. An informed and educated public will be less likely to panic, but we will have panic if we have people out there who think that they cannot get access to their medications, many of which are controlled substances.

All medication dependent Americans are looking to you for help in mobilizing national resources to help us survive. I will be happy to help in any way that I possibly can. Let us work with the RX2000 Solution Institute, the American Medical Association, the American Nurses Association, Department of Insurance, AARP, International Red Cross, any other Federal resources that we have, to prepare a coordinated national preparedness program so that the Year 2000 does not cause unacceptable deaths.

We may need legislation allowing a one-time exclusion for either Medicare, Medicaid or any other health plan to allow patients to get a 90 day supply of their medications at the end of 1999 instead of just a 30 day supply. We would then need to come up with a creative process to distribute and store controlled substances and radioactive isotopes. We need to work with the CDC, the Centers for Disease Control, to prevent global epidemics from the lack of antibiotics and immunizations.

We should compose a national patient advocacy council to monitor Year 2000 efforts within all health care organizations and provide patients and health care providers a media where they can turn, where they can look for help, where they can get answers. And if worst case scenarios occur and health care is rationed, the public needs to know which diagnoses and which procedures will be covered.

Thus far, most health care organizations are taking the position that they can reduce their liability exposure by minimizing their due diligence and their education. That may be politically correct and legally correct, but I do not consider that to be ethical. If we do not teach the patients what they need to do, we will die. There is no harm in overreacting to this issue. There is harm if we do not react.

I am willing to do whatever I can to help in any way to save as many lives including my own as possible. And my story is not unique. There are millions of people who are at greater risk than myself who need your help. And for them and for myself I am asking for your help. Thank you.

[The prepared statement of Ms. West can be found in the appendix.]

Chairman BENNETT. Thank you. May I ask you a question or two? It is my understanding that your medication is sufficiently unusual that you require a very careful calibration that involves medical devices that are something other than just pills sitting on a shelf; is that true?

Ms. WEST. To keep my tumor from regrowth, there is an oral medication that I take. My risk is with infection and in order to receive the IV antibiotics, those are at such a high concentration that in order to receive those, I have a catheter that is inserted into the antecubital vein of my arm and then threaded up into the superior vena cava of my heart, and you can only do that under sterile circumstances.

Chairman BENNETT. But the calculation of the dosage requires devices——

Ms. WEST. That is correct.

Chairman BENNETT [continuing]. Which could fail because of Y2K?

Ms. WEST. That is correct.

Chairman BENNETT. I wanted to make that clear so that everybody understood it is not just a matter in your case of stockpiling 90 days worth of pills. The device that controls this daily injection must be absolutely on in terms of its calibration and its accuracy or you would not survive a couple of days. Is that——

Ms. WEST. That is correct.

Chairman BENNETT. I do not mean to overdramatize it, but your delivery seemed a little cool, and I wanted everybody to understand exactly how serious the calibration issue is in your case and how vulnerable you are to a Y2K failure.

Ms. WEST. And there are patients who are at much greater risk than myself such as transplant patients and insulin dependent diabetics. They have less time than I have and the calibration for their medication also comes from a device with a microprocessor and in many cases those medications cannot be stored. The medication that I take for my tumor, I can store 6 months worth of that and then I rotate through that. The IV medication that I take for the infection in my head, I cannot store that for more than 2 weeks.

Chairman BENNETT. Thank you for that clarification. Do any other members of the committee have questions?

Senator COLLINS. I just want to thank you, Ms. West, for coming forward and sharing your personal experience. The fact that you have been both a clinician and a patient gives you an unusual insight to share with the committee. I wish you the best of everything and I really appreciate your taking this good out of your very difficult experience.

Ms. WEST. Thank you.

Senator SMITH. I would just simply second that. Thank you for being here and others will benefit because you have shared your story.

Ms. WEST. Thank you.

Chairman BENNETT. Thank you. You have helped us dramatize in a positive and I think worthwhile way the challenge of this. We were in a hospital yesterday, Senator Dodd and I, and some people connected with the health care industry have said to us this is not a patient care problem, this is just a computer problem where our billing system is at risk. We did our very best yesterday to make it abundantly clear this is first and foremost a patient care problem. Your being here today and your willingness to share your experience with us has helped to dramatize that for any who still have not got the message.

Ms. WEST. Can I make one more statement?

Chairman BENNETT. Surely.

Ms. WEST. I am astonished that physicians, many physicians, and many hospitals are considering this to be an IT problem only. And at this point, there is not time for a complete electronic fix. Their only alternative is for physical contingency plans working closely with pharmaceutical companies, closely with biomedical device manufacturers, to make sure that there is a continual supply or we will have large scale mortality rates in the Year 2000.

Chairman BENNETT. Our third panel will consist of a number of pharmaceutical companies. I know their representatives are in the room; that is one of the reasons why we asked you to be our first witness so they could hear this directly from you. Thank you again for coming and for sharing this with us.

All right. We will now start with Lou Marcoccio from the Gartner Group, and he will set the scene for the hearing. His research is based on a network of some 15,000 companies in 26 vertical industries in 87 countries. He will share the results of Gartner's research into the impact of the Year 2000 problem on small, medium, and large companies and the relative Y2K preparedness of industry sectors within the United States. And he will also give us an update of the Y2K status of other countries closely connected with the U.S. economy. If Ms. West gave us a laser beam micro-view of the Y2K impact on one individual, Mr. Marcoccio will give us the macro view. In some cases, it is almost as scary. Have I pronounced your name correctly, sir?

Mr. MARCOCCIO. Yes, you have, Senator, yes.

Chairman BENNETT. OK. Fine. We welcome you here and I apologize in advance when the buzzer goes off. We will do our best to run over and vote and get back as quickly as we can, but we will get started.

STATEMENT OF LOU MARCOCCIO, RESEARCH DIRECTOR, GARTNER GROUP

Mr. MARCOCCIO. OK. Great. First of all, thank you, Mr. Chairman and members of the committee, for having me here this morning to share this information with you and this important research that we have been working on and pulled together in regard to the scope and status and risks in regard to Year 2000 throughout key industries and throughout the world.

In developing our research at Gartner Group for those who do not know, I would just like to make a comment here that we do our research in several ways. We have tens of thousands of clients throughout the world that we work with everyday in all industries throughout most countries of the world. We also do surveying of very large numbers as, Senator, you mentioned, of 15,000 companies in 87 countries including the country governments and their agencies as well as far as status and specific risks related to those specific companies and government agencies.

One of the things that we find is that first of all throughout 1998, there has actually been tremendous progress and, in fact, in

1997, in calendar year 1997, about 5 percent of information technology budgets were spent on average on the Year 2000 problem and on Year 2000 projects. In calendar year 1998, that has increased by six times, and during calendar year 1998 the companies that have started and government agencies that have started on this problem are spending an average of 30 percent of their information technology budgets. Unfortunately, we have not seen as much of an expansion in other areas outside the IT area. We see now about 30 percent of companies that had previously started on Year 2000 in calendar year 1997 have expanded these efforts into other areas of business, areas of contingency and other areas of integration and interoperability between themselves, other countries, other facilities and so forth throughout the world.

What we find in our information—basically we do our surveys, we do our measurement of companies and governments through a method that we call COMPARE. It has five levels I would just like to briefly mention so that you understand when I go through the actual status. These five levels include level I being companies that are basically just getting started. They are doing awareness. They are getting people or a champion to head up the activity within a company, and they are starting to do their inventorying of both their IT systems and also their key business processes as well.

In level II is where these companies basically complete detailed inventories of their business dependencies and the remainder of their IT components, embedded systems and other things that they at least can get their arms around and identify, which in many cases is a difficult task in itself.

In level III these companies actually get detailed program plans put together, project plans, they get the resources identified, committed and in place, and they start doing the work as far as actually getting systems remediated and fixed and also doing a great deal of work as far as identifying dependencies and risks with vendors, supply chain vendors and other business dependencies. In level III, they also get 20 percent of what they identify as their mission critical systems fixed, tested and back into production environments within their companies.

In level IV, they get the remaining 80 percent of those mission critical solutions fixed and back into production as well as completing a detailed risk assessment and development of contingencies and alternatives in order to lower the risks enough in order not to have major business interruptions.

In level V, they basically complete whatever else they have time to complete outside of mission criticality as well as putting procedures and policies in place to ensure that they do not bring in infected systems or other business processes after they get their systems fixed. So those are basically the five levels.

First of all, I would like to identify status associated with size. When we look at all companies and all government agencies throughout the world, we identify size in three categories. First of all, small is under 2,000 employees. We do have some subcategories as far as extent of size in the small category, but we identify small as under 2,000 employees. Medium or mid-size is 2,000 to 20,000 employees. And large is over 20,000 employees.

What we find at the present time this quarter—in fact, as of just a couple weeks ago in our latest status survey—we find that small companies throughout the world in this under 2,000 employee category are anywhere from not started at all up to approximately the end of level II, which means that they have gotten some great extent of their inventory completed. That is the range throughout the world as far as small companies.

The mid-size companies run the range from between being about halfway through their inventory activities up to and including having as much as ten to 20 percent of their internal systems fixed and have started testing. So it is a pretty wide range on the mid-size companies as well. And the large companies, over 20,000 employees, run the range from the end of level II, which means that they have basically nearly completed their thorough inventory of business processes as well as their internal IT systems, all the way up to having as much as 70 to 80 percent of their internal systems fully remediated and are well into the test phase.

Now, this means if we were to look at actual timeframes, we find that it takes—and this is a pretty important fact to us—it takes an average of 30 months for a mid-size company or government agency to complete their systems, mission critical systems, that they identify as mission critical. That means that unfortunately it takes about 6 months under 3 years to get that kind of activity completed. That is from the time they start to the time they get their mission critical systems made compliant or at least remediated, fixed, and back into production.

Now that means that small companies, the difference between small companies and mid-size companies right now runs between—well, it is about 1½ to 2 years difference between medium to large companies. So large companies are way out ahead of, of course, small and mid-size companies overall throughout the world. It is a 1½ to 2 year difference between mid-size to large. And right now it is running 2½ to 3 years between small to large companies. So large companies are considerably out in front throughout the world and especially here in the United States.

Now, 23 percent of all companies throughout the world of all sizes, all industries, have not started as of yet on any Year 2000 activities or efforts; 83 percent of that 23 percent are small companies. That is what we categorize as small companies throughout the world.

So understanding that by size, let us now take a look by industry. According to our latest survey, we find that the three industries that are farthest out ahead are insurance, investment services, and banking. I think we are all somewhat familiar with the reasons why those industries are somewhat ahead. Basically, their mission critical systems were a lot more obvious up front or early on. In some cases these are the industries that are most regulated, and in some cases we have situations where these industries actually experienced failures starting quite awhile ago. In fact, banks had failures in regard to processing 30 year mortgages back in 1970 and so forth. So these are the industries that are farthest head.

Chairman BENNETT. They are also the industries that come under the purview of the Senate Banking Committee where Senator Dodd and I got started on this. In an election year where we are both up, we cannot fail but to take note of that. [Laughter.]

Mr. MARCOCCIO. So looking at this same chart, you can see that some of the industries that are farthest behind unfortunately are like education, health care, especially health care as far as hospitals and elderly care facilities. The oil industry is surprisingly behind in these activities. Industries like semi-conductor, food processing and agriculture, farming, construction industry, all of these industries are dangerously behind and if you look at our 30 month timeframe that it takes to get mission critical solutions compliant, they are dangerously behind in this situation.

Senator SMITH. Mr. Chairman, I notice that the lawyers are dangerously behind. Does that mean that business can sue their lawyers? [Laughter.]

Chairman BENNETT. I am sure some lawyers will figure out a way to sue other lawyers.

Mr. MARCOCCIO. Yes. And we separated medical practices out of health care because we found such a stark difference. Medical practices in general are extremely behind on this activity. We find a very small percentage have actually started any activity whatsoever in addressing the problem.

Next slide. The next item has to do with—excuse me. I am sorry. We are out of sync. We need to go back. There we go. Yes. OK. The next slide here we have categorized basically all of the industries and what we have been doing is we have actually been following failures for some time. We have put analyses together associated with being able to calculate predictions related to status, related to history of failures that have occurred in those industries and in those size companies, and we have been able to analyze and come up with a prediction associated with these four categories of industries.

As you can, the industries that are farthest ahead in category 1, we have now predicted that 15 percent of all companies in those industries will experience at least one mission critical system failure. The industries that are in category 2, 33 percent, or approximately one-third, of those companies in those industries will experience at least one mission critical system failure. And, of course, a mission critical failure means that a business interruption is likely to occur. It could affect revenue and will likely affect the continued operation of that business.

The category 3, one half of all companies in those industries throughout the world will experience at least one significant mission critical system failure. And in our last category, which is extremely severe, we will have two-thirds of all companies in that category will experience at least one significant mission critical system failure. So these are clearly the industries that are at most risk and we have gone through subcategorizations in these areas to identify risks of various severity within these industries as well.

The next item I would like to share is associated with status of countries—go on to the next major slide—the status—it is another one like that one. The status of countries we have been able to identify associated with where they stand and basically as you can clearly see the United States is definitely farthest out front when we include all sizes, all industries of companies throughout, and government agencies at both the Federal, State and local level. You can see the United States is clearly out in front. We have other countries that are just slightly behind like Holland, Belgium, Sweden; several of the western European countries are just slightly behind the United States.

Now when we look at countries that are farthest behind, you can see that we have an anomaly in Western Europe where we have Germany very far behind. Germany has had a major focus on a new monetary euro system. They have also been a major driver of that strategy and in order not to lose focus on that activity or actually lose focus on the activity, they have actually put very little effort up until now associated with the Year 2000. It has only been as of late that many industries and companies in Germany are now starting to figure out that they need to address the problem and now they are scrambling to figure out how they can get moving as quickly as possible. We also have countries like Japan that are relatively far behind.

Next slide, please. Now we have taken the countries as well and categorized them in four categories. And as you can see, we have been able to predict the percent of companies in each of these categories as far as how many companies will experience at least one significant mission critical system failure, and you can see the countries in category 1 where we will have 15 percent of those companies—and again, this is all sizes, all industries—will experience at least one significant mission critical system failure. These include countries like Australia, Belgium, Bermuda, Canada, Denmark, Holland and so forth.

The countries that are in category 2 where companies in those countries, 33 percent of them, will experience a significant mission critical system failure, and these include countries that many of our companies are well entrenched with. There is an awful lot of dependency on. Many are addressing markets in these countries to a great extent. Countries like Brazil, Chile, Finland, France, Hungary and so on.

In category 3, 50 percent of companies and government agencies in those countries will experience a significant mission critical system failure. And, of course, in category 4 we are talking about two-thirds will experience the same. So you can see the probability and the extent of the problem here; the seriousness of the problem within these countries is extreme. We find in countries like Afghanistan, Bahrain, Bangladesh, Cambodia, Chad, China and so on and so forth, we have, first of all, very little effort going on at the government level within these countries, either local, regional or federal. And we also find that most of these industries are way behind, many of them not even started in many of these countries.

What we have done is we have taken our detailed information down at the next two or three levels beyond this, this research, and we have been following not only failures but the extreme details of this status, and we have put together now an analysis, analytical analysis, associated with our predictions related to the infrastructures within these countries and what some of the likely outcomes will be. Now if we take those four categories of the countries down at this lower, bottom slide on the floor here, you can see they have been categorized across the top of this slide, and as you can see, in category 1, which the United States would be in, we have identified a situation such that we will have isolated and minor problems related to power loss. We do not see at this point in time serious or severe power loss especially across or broad-based across the United States. We see that we will have some problems. There will be some interruptions, especially down within community power companies, very small facilities and so forth, and we have categorized those as isolated and minor.

Same thing with telephone operations. Isolated and minor issues. As you can see, if were to go across to the last category of countries that are in the most severe condition, when we talk about power loss, they will experience a widespread and moderate. And these categories down at the bottom—by the way, when I say widespread, I am talking about the distribution of the failure and the problem throughout the entire country—and then the second item is associated with the severity. So we are talking about widespread and moderate situations as far as power loss, as far as telephone operations and interruptions.

And when we get to government services within those countries, we are talking about a situation where we have widespread distribution and extremely severe severity issues. The governments in many of these countries have not started any activity whatsoever in some cases. If they have started, they are way behind.

Next slide, please. So if we look at failures that are likely in each of these cases associated with these countries, associated with these industries, if we look at failures overall, what we find in our research also—and also by following the history of these failures so far—we find that a failure, any mission critical failure will cost anywhere from in a smaller company as little as $20,000, which could be extreme to some small businesses, up to $3.5 million to get themselves back operating associated with a mission critical failure. This is the range of what it will cost by failure.

Also, a key point here is that failures overall, when we talk about all these failures that will occur, 10 percent of them we are predicting will last 3 days or longer. It is likely that a small percentage will last more than 3 days, but we know that, and we can predict that 10 percent will last 3 days or longer.

Chairman BENNETT. Is that in the United States?

Mr. MARCOCCIO. That is overall, worldwide across all industries all countries. In the United States, we have also calculated and find that, yes, that holds true in the United States as well.

Next slide. Now another point I would like to bring up is one of the things that I hear all the time in working with many companies, in fact doing conferences and talking with clients throughout the world and many country governments, there is still a misnomer out there. You were talking about awareness earlier, Mr. Chairman. The misnomer is that many people think that Year 2000 failures will occur at the strike of midnight January 1, 2000, and that that is our only fear and our only threat. That is absolutely not the case. In fact, we are talking about at the actual millennium rollover, the failures that are likely to occur are related to the embedded chip failures that are likely to occur or happen.

We do find in our research, by the way, that the number of embedded chips, and we have been working with many engineering organizations, manufacturers of chips, and manufacturers of many types of equipment, we do find that a small percentage of embedded chips, a very small percentage, will fail in total. I have seen numbers publicized about 30 billion chips that we have, embedded chips throughout the world, and I have seen numbers of 10 or 20 percent that are likely to fail. Our research does not show those numbers. In fact, our research shows that embedded micro-controllers, we are talking about 1 in 100,000 as far as failing.

Now, unfortunately, that 1 in 100,000 may be running a very critical operation as far as power operation or life support system or whatever. So, of course, they have to be researched and evaluated and analyzed. But the number of actual failures we are going to see from embedded systems or embedded chips will be very small in number. But the embedded chips that do fail, however, most of them will fail at the strike of midnight, January 1, 2000. That is the way they are engineered, designed. In fact, they are engineered to monitor 8 second intervals, and within 8 seconds of that strike at midnight, those embedded chips will fail. The majority will fail.

However, when we look at computer systems throughout the world that are likely to have failures, those failures, of course, have been occurring already in low volumes for some time, through the 1970's, 1980's and so forth, and, in fact, throughout 1997 and 1998, we have had quite a few failures. The volume has gone up somewhat in regard to material resource planning systems, in regard to many devices or systems that are used to forecast information, quarterly or yearly forecasts, especially 2 or 3 year forecast information.

So in 1998, we have been seeing failures occurring. In 1999, we are expecting that the volume will go up considerably. Most companies are going to be entering their fiscal 2000 as far as their business fiscal years, and we also have many other attributes that will cause the volume to go up considerably in 1999. We will see failures go up dramatically in the Year 2000, but they are not going to just peak and drop quickly when we hit 2000. These failures will occur at a fairly consistent rate throughout the entire year of 2000. We have many transactions in many of these systems that do not occur at the strike of midnight. They occur either the next quarter or within the next segments of business throughout the entire year. And this will continue in 2001 at a reduced rate, 2002, so we are talking about a 3 to 4 year period of considerable number of likely failures.

Chairman BENNETT. I have to interrupt you here. I need to get over to the vote and we will return as quickly as we can. This is fascinating stuff and I have some questions for you, but I apologize. The committee will stand in recess.

[Recess.]

Chairman BENNETT. The committee will come to order. OK. Mr. Marcoccio, again my apologies for the interruption. We are back to your last chart, as I understand it.

Mr. MARCOCCIO. OK. Great. Well, my point on that last chart was, of course, that the failures will occur over a 3 or 4 year period as opposed to a single point in time and when we look at risks and we talk about potential effects, global effects, economic effects and so forth, we really need to be thinking about that entire spectrum or period of time as opposed to one point in time.

And my last comment that I wanted to make basically is associated with the potential risks to the United States specifically. From a domestic perspective, the risks that we have identified or highlighted as being most important are the interruptions or failures due to interdependencies and interconnections between companies and countries and we feel that can produce a considerable negative impact. Second, of course, the IT systems in critical industries that will not be fixed in time because many of these companies just will not have time because of the 30 month factor and the amount of time it takes to get mission critical systems completed. And then there are several other risks, of course, that I have in my testimony, but from a foreign perspective, the foreign business interruptions which would impact, too, many U.S. companies, of course, from a dependency perspective—foreign security issues ignited by things like unrest or severe economic issues. Many of these countries, of course, that I had in that fourth category, we are talking about the likelihood for significant impact to their basic infrastructure.

So things like foreign security, national security, as well as unrest in those countries, is very likely in our estimation. Key foreign government agencies will experience significant failures and therefore the interrelationships between our government agencies, militaries and so forth are also highly critical.

And this last point is associated with our recommendations to the committee. I guess the most primary recommendation would be to identify either a specific Federal agency or group that exists today to manage and coordinate the global impact of Year 2000. We think this is of ultimate importance. Of course, all the other issues and items that are being dealt with within the committee we feel are important as well, but we feel it needs a major focus as far as addressing the global impact issue.

And the second recommendation is associated with the Security and Exchange Commission, and I know, Mr. Chairman, I think you have done some great work in trying to drive the issue of disclosure throughout the United States as far as publicly held companies. We find in our research, however, that there is a vast amount of difference between what has actually been disclosed thus far and the actual status within the majority of companies, even here in the United States.

We do find that a lot more as far as numbers of companies do intend to at least make or fill or provide their disclosure statements in this next quarter, related to some contingency work and so forth, but we still find, even with the work that is being done today, a considerable difference in reality versus this extreme optimism. We would strongly recommend that a policy be adopted where either the SEC or another independent agency or company actually provide a set of random audits associated with these companies. As we all know, this process works at least relatively well as far as our IRS and our tax returns, and we feel that that is definitely necessary in order to get these disclosures much more accurately implemented.

And last, the recommendation I would like to bring out is associated with new legislation that is implemented. We would like to see all new legislation questioned as far as determining if it may require IT modifications and systems. There is an awful lot of legislation that is launched that requires in many of these industries we are talking about being far behind—education, health care and many others—to go and make changes in their systems related to reports, related to regulations and other types of changes. We would like to see an evaluation be made or at least some kind of quick assessment be made on any of these pending legislations and that we would ask that these types of things as much as possible be put off or stopped because we are basically adding to the serious condition—the fact that they have to go out and spend critical time implementing those changes.

Last, we would like to also recommend that we set correct expectations within the U.S. Government agencies and also any other awareness activities that comes out of the committee associated with the period of time that these failures will take place. We find even in reports and documents from our U.S. Federal agencies that there is a misnomer associated with the period of time that these failures are likely to take place. So we would hope that some effort be put in place to accurately make aware individuals and within our Federal agencies that we are talking about a much longer period of time for potential failure and risk.

[The prepared statement of Mr. Marcoccio can be found in the appendix.]

Chairman BENNETT. Thank you very much. I have a whole series of questions I would like to sit down and discuss with you and we could take all of the rest of the morning with you. Unfortunately, we do not have that time. And the Senate vote has eaten up half an hour or more of our time in addition. Let me ask you if you would be willing to respond to questions in writing that would be made part of the record?

Let me just pick out several of the things you have said in your testimony. You talked about 1 to 3 days being the duration of some of these problems. Thus, I think the implication in some people's minds is, OK, the problem will hit and we will have 3 days to solve it and then it will be over with. And that brings to mind the statement by one nuclear physicist in Russia who said we plan to do nothing about Y2K. We will just let it come. When it hits, we will see where the problems are, and then we will buy the fixes from the United States. So that is the easy way to deal with this.

I want to give you the opportunity to correct the impression that no matter how bad it is, it can be fixed within 3 days.

Mr. MARCOCCIO. OK. Well, we do do a pretty thorough analytical analysis associated with that information, but one point I would make in regard to that would be that since we are talking about many millions of failures that will take place and even mission critical failures throughout the world, when we talk about all failures in the millions, 10 percent of those will last 3 days or longer. That is extremely substantial in our mind to have 10 percent of a very, very large number last 3 days or longer. We are talking about business interruptions where a factory that runs three shifts a day may not be able to operate for 3 days or longer. We are talking about situations where goods that may have a very short shelf life not be able to be delivered within 3 days. We are talking about very, very substantial unfortunately ramifications associated with that 10 percent.

So I by no means meant to lighten the situation with the 10 percent, but when we look at the real numbers, the likely number is in the millions throughout the world of total failures. Yes, 10 percent will last 3 days or longer is likely to occur and what we are predicting. We feel that is a very, very large number. We also feel a percentage of that will last 15 days or longer as well. In many cases, if you are talking about extreme conditions, if you are talking about basic infrastructure, very large corporations, to have a failure and a business interruption and a large portion of a business actually shut down that operation for 15 days or longer we feel is a very, very serious and severe situation. So, yes, I did not mean to make that sound like a very light statement. We feel that is pretty severe.

Chairman BENNETT. Yes. No, I know you did not. And that is why I gave you the opportunity. I come back to this chart that says 4 years. We have to look at the macro world in terms of the lasting impact of this thing dragging out over that period of time.

Now, back to your chart on the level of readiness in various countries. I have the feeling that some countries will simply drop off the radar screen and may be there. That is out of sight in terms of their ability to connect with the world for several years. Is that a correct?

Mr. MARCOCCIO. I think that extreme situation is possible in some cases, yes.

Chairman BENNETT. And if that is a country where we are—we, the Western world, not necessarily just we the United States—taking critical materials, the interruption of that supply chain will cause enormous repercussions. The Western world will not stand for an interruption for several years and will find alternative sources of supply. Therefore, the country that is just beginning to build itself up economically on the basis of whatever it is they produce suddenly finds themselves wiped out of its ability to compete. The desire of industrialized nations to have alternative supply sources turns them to their competitors. Even if they then get their Y2K problem solved, they are so far behind the market they cannot ever climb back into a competitive position. As a result we will have a serious humanitarian problem; CNN will go in with their cameras and show starving children. Last time CNN showed starving children in Somalia we sent in troops, and I think we are going to have other aspects of that in various countries around the world as a result of this problem.

Now am I overstating it? Do not hesitate to disagree with me. I am not trying to make a political point here. I am trying to get information. If I am overstating it, tell me and tell me why.

Mr. MARCOCCIO. No, I think that situation is definitely possible in some number of countries. Some of these companies basically that are in that fourth category have situations where they have dependency within their government agencies. Many of the countries in that category, basically the country owns the power company, the telecom company. In some cases, we are talking about food distribution being heavily owned or supported by the government. We are talking about situations where we already have close to or at starving situation of people and food. We are talking about countries where we already have some unrest occurring.

Considerably, in many of those countries, we are talking about situations where they have threats between their country and others from a national security perspective. So we already have a pretty significant situation, even from a global economy perspective as well with those countries, and this is going to add considerable turmoil to those countries and in some cases may do exactly what they said and actually may shut them out of any type of global market opportunities.

Chairman BENNETT. OK. Thank you very much. I have many more questions I would love to discuss with you.

Mr. MARCOCCIO. We would be glad to submit answers in writing or follow-on meetings or whatever.

Chairman BENNETT. All right. We will do that, but in the interest of time I will turn to Senator Smith.

Senator SMITH. In the interest of time, I will just submit written questions.

Chairman BENNETT. OK. Thank you again, and our apologies for the interruptions. It has been very useful.

We would like now to hear from the Honorable Fred Hochberg, Deputy Administrator of the SBA. We had planned to have him on a panel with a number of other witnesses. Mr. Hochberg, given your time pressures, I think we will hear from you first and ask you your questions and then hear from the other members of the panel. Again, we apologize to you. I think you probably would learn from the questions and answers from the other members of the panel. So we invite you to stay as long as you can, but we do understand the pressures that are on you and we will hear from you now.

STATEMENT OF HON. FRED P. HOCHBERG, DEPUTY ADMINISTRATOR, SMALL BUSINESS ADMINISTRATION

Mr. HOCHBERG. Thank you. Thank you, Mr. Chairman, for inviting the U.S. Small Business Administration to testify before your committee. My name is Fred P. Hochberg, Deputy Administrator of the SBA. I appreciate the opportunity to discuss the Year 2000 or Y2K problem facing the nation's 23.6 million small businesses. Before I begin, I would like to applaud both you, Mr. Chairman and Vice Chairman Dodd, for your leadership on this issue. I would ask that my full statement be made part of the record.

Chairman BENNETT. Without objection.

Mr. HOCHBERG. As someone who has run a small business and met a payroll, let me assure you I know firsthand how potentially disruptive the Y2K bug may be to a business. We at the SBA are committed to doing all we can to minimize the impact of the Y2K problem on America's small businesses. To some extent all small businesses may be affected since any firms with non-Y2K compliant hardware, software or equipment with time-dependent chips are potentially at risk.

And small firms should not forget their dependence on outside entities. A business that has addressed its Y2K issues in-house could still suffer or fail because a key outside firm with its own Y2K problem fails to perform. However, it is clear that with foresight and preparation, the problem can be avoided or at very least minimized.

In July of this year President Clinton issued a challenge to both the private and public sectors to work together to address this critical issue. The President's Council on the Year 2000 Conversion under the dynamic leadership of John Koskinen has spearheaded the administration's efforts in dealing with this problem. Let me briefly update you about what the SBA is doing to ensure that our own computer systems are Y2K compliant and what SBA is doing to help our customers.

With regard to SBA's internal computer systems, I am pleased to inform you that as of today we have completed the renovation of the computer programs in all of SBA's mission critical systems ahead of the targeted goals for the Federal Government.

Let me now turn to discussing how SBA is striving to help the nation's small businesses cope with the Y2K issue. Our goal from the beginning has been to bring the seriousness of this problem to the attention of the small business owners without creating undue panic. As a result of our work with industry experts, we have developed a common sense three-step program that anchors our Y2K outreach efforts.

First, businesses are encouraged to conduct a self-assessment to see if they may have defective computer hardware and software as well as any equipment using date sensitive embedded computer chips.

Second, businesses are encouraged to take action immediately. Now is the time to begin evaluating and addressing one's vulnerability to the Year 2000.

Third, businesses are encouraged to stay informed about this issue. Accurate Y2K compliance information could change and business owners need to keep abreast of any modifications they may need to make as a result of changes in their business operations.

Part of this process also includes following up to ensure your suppliers and distributors are Y2K compliant and developing contingency plans to deal with problems that may arise or are beyond their control. These three steps form the basic message of our public awareness program. We have prepared a series of materials and services to notify small businesses about the Y2K issue. They include the posters you see in the room, fliers that we are putting in bill statement stuffers such as this one, a toll-free hotline, a special Y2K section of our website, the address of which is www.sba.gov. In fact, since its inception in February of 1998, this site has been hit or visited over 840,000 times.

Our traditional resource partners have been a tremendous asset in helping us spread the word about Y2K. Since our Y2K kickoff in early June with you Chairman Bennett and Vice Chairman Dodd, the SBA has conducted Y2K training events throughout the country. Since June, we have distributed more than two million of these fliers through our private sector partners such as financial institutions, utility companies and newspapers.

We are also very excited that recently we reached an agreement with the Internal Revenue Service to distribute nationwide 6.5 million of these fliers to small business owners.

Before I conclude my testimony, let me tell you about an exciting activity we have planned for later this month. We will sponsor a nationwide Y2K action week during the week of October 19 to focus government, business and media attention on the Y2K problem. We have nearly 340 events already scheduled across the country in conjunction with this effort. I am also happy to report that 47 of those events are in States that members of this committee represent. It is our hope that we can reach millions of small businesses and motivate them to take action now on this critical issue.

Let me conclude by saying the bottom line is small businesses need to take action now and stay informed on this issue. It is too late to start early. The reaction to our efforts has been overwhelmingly positive. As you return to your respective States in the coming weeks, we urge you to carry forward the Year 2000 message. You are uniquely situated to bring the urgency of this message home to the small business community. We frankly need your help in this effort and would be happy to provide materials or help you communicate with your small business constituents.

For most businesses, the Y2K issue can be managed if they take action now while there is still time. Thank you, Mr. Chairman, for inviting the SBA to testify. I look forward to working with you and would be happy to answer any questions.

[The prepared statement of Mr. Hochberg can be found in the appendix.]

Chairman BENNETT. Thank you very much. We applaud what you have been doing. I note that John Koskinen has helped you in changing the title of Y2K Awareness Week to Y2K Action Week because if we are only dealing with awareness we are too late.

Mr. HOCHBERG. Exactly.

Chairman BENNETT. You are aware, I am sure, of the study that was done by the NFIB in conjunction with Wells Fargo Bank, in June or July where 82 percent of small businesses said they had no Y2K plans and, more chilling for me, 40 percent or roughly half that number said they did not plan to get any Y2K plans. Now you have done yeoman work in trying to get the word out. Do you have any statistics that could be used to counter those summer numbers to say that the percentage of small businesses that are now going to try to deal with this might be going up or do we just have the number of hits on your web site and a general feel that things are better?

Mr. HOCHBERG. We have not conducted research in terms on the extent of the problem. I believe NFIB has done so and has some updated information on that.

Chairman BENNETT. Good. We will hear from them next.

Mr. HOCHBERG. But we are mounting this campaign and organizing many events the week of the 19th to make sure we do get this message out. I was a small businessman. I ran a catalog company, and I understand you deal with the upcoming season, how to get inventory in, and deal with payroll issues. It is harder to get a small business person to focus on something that seems like an eternity, 15 months away. We have mounted this effort because we know there is that potential problem.

Chairman BENNETT. I understand exactly having run several small businesses myself. May I inject a somewhat cautionary note? I am delighted that you are reporting that your mission critical systems are remediated and you are going to be in good shape. Here in the Senate, we have gone through the process of trying to make sure that the Senate computers are compliant, it would be very embarrassing for me if I am out here sounding the cry for all the rest of the world and my own computers do not work. I have found that the first reports of getting things under control are almost always more optimistic than the fact. And I would really be very stunned, very pleased obviously, if all the PC's on everybody's desk at the SBA were ready. I have a suspicion that maybe that is not the case.

So I would just suggest to you as the top manager, now that you have gotten your optimistic report, go back and start asking some troublesome questions, and I think you will discover that some people said, oh, well, we did not mean that. And just as I want to avoid the embarrassment of having the Senate not be Y2K compliant all the way through, you want to avoid the embarrassment of having the SBA not be compliant. There are certain of our colleagues that I would just as soon not alert. [Laughter.]

But we will let that one go by. Senator Smith.

Senator SMITH. Mr. Hochberg, thank you for your testimony. I understand the SBA will be guaranteeing 50 percent of the loan value up to $50,000 to help small businesses pay for Y2K fixes. Can you characterize or project how quickly the guaranteed funding will enable small businesses to complete remediation and testing efforts? Do you have a sense of timing on that?

Mr. HOCHBERG. Senator Smith, all of SBA's loan programs currently are available for Y2K remediation—from our LowDoc and SBAExpress programs that were just expanded last month and through our regular 7(a) and 504 loan programs, which are for larger amounts, up to $750,000–$1 million respectively. They are all available to be used for these efforts. And our newly expanded programs, the LowDoc, standing for low documentation, and SBAExpress allow 36 hour approval times. They are very quickly available so that should not be an impediment to a company getting the funds, and those loans can be paid out 5, 10, or 15 years to amortize the cost of those changes.

Senator SMITH. Are you getting many people seeking loans for this specific reason?

Mr. HOCHBERG. Our loan programs are loan guarantees. So, in fact, we often do not see the precise nature of some of those loans. But our banks are alerted to that. In every forum that our district officers speak in, we make sure people are fully aware that these programs are available.

Senator SMITH. Do you notice banks pushing small businesses to make sure their customers are Y2K compliant?

Mr. HOCHBERG. The banks have been some of our best partners. The American Banking Association, in fact, took our entire training and education program and incorporated it into their documents. Nations bank and Wells Fargo are actually distributing this to their customers and working with other banks to do so as well. So the banks have been, as the gentleman from the Gartner Group indicated, at the forefront and I believe small businesses do listen to their bankers.

Senator SMITH. Thank you very much. I guess bottom line there is really no reason people should not be doing this in small business. They just solve the problems if they are aware of it. I do not imagine that for most large companies the Y2K problem would be a large financial hit, but it potentially could be if they do nothing about it. So thank you for your efforts.

Mr. HOCHBERG. Certainly.

Chairman BENNETT. Thank you. And you are more than welcome to stay or if you have to leave, we will understand.

Mr. HOCHBERG. Thank you.

Chairman BENNETT. We will now have the other members of the panel on small business join us: William Dennis, senior research fellow at the National Federation of Independent Business; Mr. Rod Rodrigue, director, Manufacturers Extension Partnership from the State of Maine; and Mr. Harold Schild, president/CEO of Tillamook Cheese. And I have eaten Tillamook Cheese so I can endorse the comments of the Senator from Oregon with the caveat that Cash Valley cheese in Utah is of equal quality.

All right. Mr. Dennis.

STATEMENT OF WILLIAM J. DENNIS, JR., SENIOR RESEARCH FELLOW, NATIONAL FEDERATION OF INDEPENDENT BUSINESS

Mr. DENNIS. Being originally from Wisconsin, I am going to have to argue with that. But thank you very much, Mr. Chairman. The bulk of my testimony today will be a report that was produced.

Chairman BENNETT. Yes, and it will be without objection included in the record.

Mr. DENNIS. Data for the report were collected in April, late April. We will update that report later this month. In fact, I had a conversation yesterday with the Gallup organization so we are about ready to go in and essentially repeat what we did earlier. My judgment is that the October-November data will be much more optimistic or encouraging than was the spring's. However, I say that from experience rather than data. Many small business owners, as you are well aware, have immediate pressing problems and those tend to go right to the top of the list. So the current status is not totally unexpected although not always totally understandable either.

Chairman BENNETT. Can you pull the microphone a little closer to you?

Mr. DENNIS. Surely. Is this better?

Chairman BENNETT. Thank you. Yes.

Mr. DENNIS. The critical finding in the spring report was that over 80 percent of the small businesses in this country are potentially exposed directly to a Y2K problem. To take it a little bit further, think of dividing the small business population into fifths. A fifth of them does not understand that there is a Y2K problem. They are not aware of it. A fifth are currently taking action. A fifth have not taken action, but plan to take action. Two-fifths are aware of the problem and do not plan to take any action prior to the Year 2000.

If we put together the people who do not have computers or embedded chips as well as those who have taken action and feel comfortable, we have approximately 40 percent of the small employer population. At the other extreme are those which plan to take no action, and who are computer dependent to the extent that if they lost their computers or the computers malfunctioned, would lose 85 percent or more of their production or sales. That effectively means they would have to close down for a period until they can fix it. About 330,000 businesses fall into that category. If you cut the amount of computer dependence somewhat, then you about double the number. So we have a serious problem among a significant number of businesses.

Aside from the general liability issues that you have talked about on other occasions and an assumption that the credit markets do not go south on us, it seems to me that the primary function or role of the Federal Government other than taking care of its own house is to serve as the village nag. It would be helpful quite frankly, and many of you are doing so, to——

Chairman BENNETT. I have been called a lot of things, but—[Laughter.]

Go ahead.

Mr. DENNIS. One of the critical points is to nag the right people. Let me refer you to a study conducted by the Small Business Administration in 1994 titled "How Small Businesses Learn." That study focuses on how government can communicate with the small business population. There are two key groups. The first key group are trade associations, but specifically industry-specific trade associations. The reason that they are critical is not only because they have good contact with small business owners, but because they also are aware of the equipment that is used within those industries. It is the kind of information that someone interested in smaller firms or knowledgeable about smaller firms in general would not necessarily have. So industry-specific trade groups are very important because of what they know and because they have enormous credibility within the population itself.

The second group that has enormous credibility within the population itself are colleagues and business associates. You spoke earlier about banks and their relationships and indeed they have been out in front from what we have seen. But there are other types of organizations as well, large and small, which would do well to impress upon their customers and suppliers the need to be Y2K compliant.

The upshot is that government would do well to focus on its bloody pulpit function and this it can do quite well. Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Dennis can be found in the appendix.]

Chairman BENNETT. Thank you. Mr. Rodrigue.

STATEMENT OF ROD RODRIGUE, DIRECTOR, MANUFACTURERS EXTENSION PARTNERSHIP, STATE OF MAINE

Mr. RODRIGUE. Thank you. Senator Bennett, Mr. Chairman, and Senator Smith, I am here today from the great State of Maine to hopefully bring across more solutions than problems. I am president of the Maine Manufacturing Extension Partnership, which is part of a national Manufacturing Extension Partnership, put together by NIST under the Department of Commerce. Our primary mission is to help small and medium-size manufacturers become more globally competitive by using the best available technologies.

We are the folks in the trenches that talk to these manufacturers and try to find out what we can do to help them. What we have done in Maine and the reason we have been asked to come here today is to tell you a little bit about what we have done as a model program. When we saw all the great number of manufacturers that could potentially be affected by Y2K, we got very nervous about what would be happening to our manufacturing base in Maine. With 2,500 manufacturers in Maine, 88 percent of them hiring below 100 folks, we started to look at these manufactures as the ones that were the most at risk.

A few months back NIST came out with a Y2K assessment tool. This tool is a mechanism you can hand to manufacturers enabling them to actually do an assessment of all of their inventories. It looks at the supply chain, and allows them to look at their embedded systems. For just 1 second, if you could, just visualize a manufacturing facility with 50 or 60 machines from a dozen different countries all with embedded chips networked together out of customized software, not knowing who put in the custom systems in some cases. It becomes very complicated. We have seen so much apathy with small manufacturers that we decided to call every manufacturer in the State of Maine. We estimate 500 to 600 will need help.

We took this Y2K tool and linked up with SBDC's, SBA folks, business visitation folks and so forth, and will deliver this tool to every single manufacturer that needs it on a personalized basis. We have heard today about the apathy and it really is there, but once a manufacturer uses this tool and complete their system inventory, lights come on and the manufacturers understand the value in going through an assessment.

The real back breaker in this whole process is proceeding from the awareness to the remediation phase. They cannot get their arms around the remediation problem. This process gives them a road map. At the end of this engineering road map, the mission criticals are identified and prioritized. We attach a SBA LowDoc loan application instruction sheet that gives them not only the means, but a mechanism. Then we take and help them through their remediation process.

The real good news is that this document, this tool, sits in the hands of about 2,500 MEP folks all around the country. There are 400 offices in all 50 States and Puerto Rico. They are affiliated with 3,500 other agencies that can help distribute the tool. What we are doing in the State of Maine we think would be a good model. We will continue to talk about Y2k awareness and put the action together. We have handled about 50 companies so far.

In your letter you asked me what it is the Government could do to assist in the situation. In Maine we have begged and borrowed and tried to put this product out on limited resources. With the lack of funding we will probably stop at about 100 or 120 companies. MEP has yet 400 other companies to assess. The national NIST program, the MEP program has submitted a request for funding through the Department of Commerce. I am asking that Maine's Y2K model program and the budget request be used to put this tool in the hands of all of the States in the union, allowing immediate delivery of this tool. Remembering that this is an assessment tool, we need to be mindful that manufacturers are looking at a narrow window of opportunity to complete and start the remediation process to be Y2K compliant.

What we are asking today, I guess, or what I am asking today is to have this committee reach out and plug in this system and let us go out and actually start to do the work. I did not want to bore you with more statistics of how bad it is going to be. I want to say that we can go out now and start to cure this problem. The tools are there. The people are there. I am reminded of my first job where my first boss said do not bring any more problems, just bring solutions. I am hoping that is what I am doing here today, bringing you some solutions that make some credible sense.

The national MEP system over the last 6 years has really been at the forefront of giving technology to the small and medium-size manufacturers in battling this global competition. We are in place, we are ready to go. We have the tool to go out and implement it. The bottom line for me, is to ask you to expedite or help us get the resources, the financial resources, to go forward with this program.

I want to point out that these resources we are asking for is not to pay for the remediation process. It is to help promote more awareness and alleviate the existing apathy. We are ready to go and I just hope that you will help me step on this millennium bug and finally get it out of our hair. I would be more than happy to answer any questions and I thank you for inviting me.

[The prepared statement of Mr. Rodrigue can be found in the appendix.]

Chairman BENNETT. Thank you. Mr. Schild.

STATEMENT OF HAROLD SCHILD, PRESIDENT/CEO, TILLAMOOK CHEESE, INC.

Mr. SCHILD. Schild. That is fine. Thank you. Chairman Bennett and Senator Smith, I want to thank you for providing me an opportunity today to share our experience as a relatively small farmer-owned dairy cooperative in dealing with the Year 2000 computer problem. We were first made aware of the problem back in February of 1996 during a routine annual audit by one of the Big Five firms, and at that point, we authorized Management Information Services to research the validity of the potential for problems in our computer systems. They reported that, indeed, there was a real danger of complete calamity when January 1, 2000 rolled around and that we should begin immediately toward correcting the problem.

Now, Tillamook County Creamery Association is 150 member dairy cooperative. We are nestled between the Coast Range Mountains and the Pacific Ocean, about 75 miles west of the Portland, OR metro area. The association has about 400 employees and we have sales of about $160 million per year. We are totally branded, value-added dairy products, primarily cheddar and premium ice cream.

At the time we became aware of the Y2K problem, we had an MIS staff of two people. Despite our efforts, we have been unable to attract additional staff to our coastal area to cope with everyday programming demands plus deal with the Y2K bug in addition to their daily responsibilities. Many other companies in the metro area that are able to pay higher salaries have engaged most of the qualified programmers in the region.

Our approach was to form teams that would think of all the potential problems in their areas. Some of our people were sent to seminars to gain better understanding in where to search for the Y2K bugs. A few of the potential problem areas they found, of course, were our accounting software, electronic data transfer between our order desk and our customers, member and employee payroll, quite an important area, point of sale programs. We have a visitors center that hosts about 900,000 visitors each year, and that, of course, was a real critical area for us as well as our farm store and dealing with our members.

A question about our suppliers—were they going to be compliant and able to continue to supply a regular flow of product to us? Were there legal issues? Questions we did not have answers for. Were we in jeopardy of defaulting on some of our contracts and agreements. Financial transactions. Were customers' payments going to come through in a timely manner? Was our order reception and processing going to be up to date? Were we going to be able to accept customer orders on a timely manner and get the product to them as expected?

And, of course, our automated product processing. We have a fairly modern cheese plant and processing, and we are concerned with the program controllers that actually operate that system. To date, our accounting department estimates that our out-of-pocket cash expenditures will exceed a million dollars to avoid a major Y2K problem. This does not include any of the internal costs of staff time or expense for training. The loss of productivity internally because our people are busy with Y2K issues is also not included in this cost estimate. These costs will be directly borne by our dairy members, many of whom are struggling to make ends meet already.

At the present time, we are applying a test program to all of our software to determine just where the bugs are hiding. We are confident that TCCA will be Y2K ready before the fall of 1999 if we do not experience delays in receiving software. We have contracted for the installation of this software by April 1, 1999. And we expect no problems, but then I am sure there will be some surprises. There always seem to be.

Looking at the rest of the industry, many of the CEO's of dairy companies that I talk to express a wide range of views on Y2K—from disbelief that it is more than a computer industry hype to stimulate business to a view that the electronic world as we know it today will cease to operate, leaving commerce stalled, utilities shut down, and only hand operated equipment functioning. Some project no additional costs to complying with Y2K while others estimate their costs like ours will run into the millions.

As in many other industries, the large, well financed seem to be better prepared than those who are less sophisticated and more personally operated. I would rate the dairy industry generally to be at level II in the previous testimony for overall preparedness. Items that I would suggest perhaps Congress could help us on is that many persons still are not aware of the real potential for disaster that exists. This committee is an excellent vehicle toward a broader awareness level nationwide, and I compliment you for your efforts on this behalf.

Some suggestions that could possibly help—Congress could act on—would be to establish a centralized government sponsored web page for all companies to log on to and to certify that they are completely compliant. Other companies then could access this page to verify if their suppliers and customers are prepared to function after January 1, 2000. This would reduce duplication of efforts.

Also, immediate tax recovery of all program upgrade costs. I understand that IRS has stated that a portion of any new software or hardware needed for Y2K compliance could be expensed in the current year. However, much of the software and hardware needed to operate the new upgrades will not be immediately deductible because it is not used solely for Y2K but may incidentally improve other non-Y2K functions of the operating systems. This upgrade must be expensed over a long period of time under the current IRS guidelines.

I would say at this point that we are probably doing about 5 years worth of software and hardware upgrades, all within the fiscal year 1999, in order to cover the Y2K bug. We normally would spread this over a longer period of time.

Third, if Congress could assure those of us in industry that government services will be fully compliant. I understand there is many Federal, State, and local public bodies such as utilities, emergency services, financial institutions, and transportation services that are not Y2K compliant and claim they do not have the resources to become compliant by January 2000. I thank you for this opportunity to express the Y2K status of our cooperative in Oregon and hopefully it will help others avoid a major crisis just 65 weeks from now.

[The prepared statement of Mr. Schild can be found in the appendix.]

Chairman BENNETT. Thank you very much. This has been useful to get this range of information. Unfortunately a pattern is being repeated here that we have seen in other hearings which is that the witnesses we get before us are the witnesses who know what they are doing. And they give a false impression that things are better than they really are because the witnesses that do not know what they are doing refuse to come forward. So the good ones are here and we recognize you as being representative of the good ones. The others raise great concern for us.

Mr. Dennis, you have talked about trade associations and other colleagues and associates and you highlighted banks. Do you have the sense that banks, credit unions and so on, those gatekeepers of credit, are starting to make this a loan issue? That they are beginning to say you cannot get a loan because we think you will not be able to pay it back because you are not going to be Y2K compliant?

Mr. DENNIS. Let me separate those two, Senator.

Chairman BENNETT. Yes.

Mr. DENNIS. In terms of obtaining loan money to become compliant, my sense is that is not an issue right now.

Chairman BENNETT. Yes.

Mr. DENNIS. We are in a situation now where credit is probably as easy to get for a small business owner as any time in the 23–24 years that I have been researching small firms. So I do not see that as an issue. The other portion of your question, are banks requiring Y2K compliance before they are issuing loans, I do not have a sense that that is a requirement at this juncture. I do have a sense that they are sending out letters to their—well, I do not have a sense—I know they are. A lot of banks are—are sending out letters to their loan customers which very specifically asks them about their Y2K activities and infers that it would be well if they took immediate action to remedy this problem. They are couching the inquiries in terms of having to do business back and forth over the wire, not necessarily with you, but with other people. Therefore, it should have all of its customers in compliance.

Chairman BENNETT. Mr. Rodrigue, your body language said you had an answer to that question.

Mr. RODRIGUE. Well, like I said, we are in the trenches, Senator, and they are starting to get very nervous. The bankers are sending letters inquiring about Y2K compliance. Credit terms and availability could potentially be affected.

I should mention that by the use of the Y2K tool, gives them a due diligence document so they can show the banks that they have gone through an assessment. It is another big plus. This tool not only gives them a due diligence at the end of it, it allows them to move forward because it gives them a document that tells them how much resources they need to go through remediation. But the banking portion, Senator, is a very big concern, and I think that we are going to see a little more of a panic as the months roll by.

Chairman BENNETT. I am privy to the actions inside a major bank where the credit officers are saying we did not think this was a credit issue. We now decide that it is a credit issue, we think we are going to lose between 5 and 20 percent of our customers by our action. That is we will cut them off as bad credit risks on the basis that they do not have sufficient remediation in place. Therefore they are going to start holding credit and loan officers within the bank, accountable for the kinds of loans they make with respect to this issue. This is just one bank. However, I think it is a fairly significant signal to send to small business people when they go in for a loan in May or June 1999 and be told by the bank I know we have served you for 10 years, but we are not going to make this loan because we do not think you are going to be able to pay it back.

And that raises an issue I will say here and probably repeat later on: One of the results of the Year 2000 problem is going to be a flight to quality. The banks will move to the quality loans, let other people fall by the wayside. Suppliers will move or companies will move to quality suppliers; the ones that are more marginal, they are willing to take a chance on, will be in difficulty. And as I indicated with the testimony from the Gartner Group, whole countries will be affected because people will move to quality and they will go to reliable sources of supply. It can be for a small business an opportunity to become a source of quality and thereby step up over competitors who are not paying attention to this. It can be an opportunity rather than a disaster.

One quick question for you, Mr. Dennis. NFIB, as I understand it, does not have Y2K as a mandate yet. Are you planning to take a more aggressive stand on this in terms of leadership for your members on this issue?

Mr. DENNIS. It has been featured in our magazine, websites, links to other websites, and that sort of thing. I am not exactly sure what you mean by a mandate. I am a little bit confused by that. I am sorry. We clearly have done several things on the communication side and plan to do more, but——

Chairman BENNETT. Yes. I am told NFIB members vote to put an issue on the top priority list or priority attention mandating what the staff will do and that has not yet happened.

Mr. DENNIS. Yes. No.

Chairman BENNETT. I am encouraging you to have that happen.

Mr. DENNIS. Thank you, yes. The liability issue has already been out.

Chairman BENNETT. OK.

Mr. DENNIS. And I would expect if that is on the voting side, yeah.

Chairman BENNETT. OK. Fine. Senator Smith.

Senator SMITH. Thank you, Mr. Chairman. Harold, we actually had considerable difficulty getting other food processors here and I wonder if you can conjecture with me why that might be. Is there a lack of awareness of it, not just the dairy industry but generally vertically and horizontally in the food processing industry? What do you think the awareness is?

Mr. SCHILD. I think probably the food processing industry, especially your smaller ones, are more manual and they do not recognize outside of their own daily operations the impact that it could have on them when it comes to customer suppliers. We feel that we are moving into becoming a little more sophisticated with our customers in electronic data transfer and so on, and I think our customers have probably been encouraging us. In fact, we are getting letters regularly now that demand that we acknowledge that we are compliant and or when we will be, and if that does not happen, then they threaten to go to another supplier for their cheese.

So I think maybe some in the agricultural arena are not perhaps as connected electronically with some of their customers and may not be feeling the pinch. I think in Oregon especially we have many commodity producers. I believe only about 15 percent of our agricultural sales in Oregon are actually to the end user. And therefore being more commodity driven, they are not likely to be dealing with the end users that are really demanding this level of compliance.

Senator SMITH. Could a component of it be fear of being associated with bad news?

Mr. SCHILD. Well, there is probably some of that.

Senator SMITH. Is legal liability part of it?

Mr. SCHILD. I guess that has not bothered us.

Senator SMITH. Well, actually I think there is a competitive advantage to be marketed in some way to let your customers know you are Y2K compliant and you are on the bridge of the 21st century.

Mr. SCHILD. Well, we are certainly working that way and we are confident that we will be ready. But we still have questions. In fact, we are preparing the same compliance letters with many of our suppliers to make sure they will be able to serve us after Year 2000. So it goes around.

Senator SMITH. I thank you for coming and for sharing with us and I hope that all of you will continue to do what you are doing. We appreciate it. Thank you, Mr. Chairman.

Mr. SCHILD. Thank you.

Chairman BENNETT. Thank you very much. We appreciate your being here. I will make this comment following up on Senator Smith's comment. I have been in touch with some of the trade associations in the food industry and made it as courteously clear as I can that we will have representatives of the food industry testifying next year. We have the subpoena power on this committee. We have not had to use it up until now and I hope that the time never comes when we do, but one of the main concerns that the public has, particularly in some of the more alarmist websites with respect to Y2K, is whether or not there will be food on supermarket shelves. Many people are saying there will not be, and I have said to representatives of the food industry if you wish to allay this suspicion and convince people that food will, in fact, be on the shelves in supermarkets on January 2 or 3 and it will be freshly delivered food, you had better come before the committee in making your case. Your unwillingness to come and share information with us only feeds the people who are pushing the panic button.

So we will have representatives of the food industry before us at hearings next year. Another reason, Mr. Schild, why we are grateful for your coming. You are willing to go whether others never dared to go before. [Laughter.]

We are glad to have you here. Thank you, all.

Mr. RODRIGUE. Thank you, Mr. Chairman.

Chairman BENNETT. We will go now to the final panel. This panel is flying two missions. They represent big business. We have had the representatives of small business. Now we are going to hear from the representatives of big business. And at the same time they are all concentrated in the pharmaceutical industry. So we will be able to get the kind of sense of availability and Y2K compliance in that key industry as well as get a sense of what large companies are doing.

I think it is fitting that we started out with Ms. West who gave us the very graphic and moving description of how important this industry is, and now we finish up with the pharmaceutical industry. I am sure you all heard her testimony and we look forward to learning how you intend to address the problems that she raised, at least from your part of this particular supply chain.

We have with us Dr. Charles Popper, who is the chief information officer of Merck & Co.; Mr. Keith Mallonee, who is vice president of Information Technology at McKesson Corp.; Mr. Ronald J. Streck, who is the president and CEO of the National Druggists' Association; and Mr. Richard Carbray, who is the general manager of a small pharmacy, Pelton's Pharmacy an Home Health Centers.

Let me make one other comment. Senator Dodd was involved in a fender bender on his way in this morning and while there is nothing dramatic about it, he has got a sore neck. He is trying to get a little bit of relief and that is the only reason he is not here. Senator Dodd is usually the most faithful of all members and please do not misinterpret his absence as any kind of lack of interest. His written statement will be included in the record.

[The prepared statement of Senator Dodd follows:]

Chairman BENNETT. So I see you have seated yourselves differently from the way I have it listed. Let us go in the order that you are seated. We will start with you, Dr. Popper, and then Mr. Streck, Mr. Mallonee, and Mr. Carbray.

STATEMENT OF DR. CHARLES POPPER, CHIEF INFORMATION OFFICER, MERCK & CO.

Dr. POPPER. Thank you, Senator Bennett. Good morning, Mr. Chairman and members of the committee. My name is Charles Popper and I am Vice President of Corporate Computer Resources at Merck. In that position I serve as the chief information officer of Merck. Merck is a global, research-driven pharmaceutical company that discovers, develops, manufacturers and markets a broad range of medicines. Thank you for inviting me to participate in today's hearing. I applaud this committee's efforts in both investigating and publicizing the potential effect of the Y2K computer problem.

I would like to discuss what my company, Merck, is doing to deal with the problem. I would also like to provide a broader context that you may find useful. Our task at Merck has been to ensure that all computer programs that are in use anywhere within Merck's worldwide operations will operate correctly throughout the transition into the next millennium, but our objective all along has been a more important one consistent with Merck's company mission. As George W. Merck stated many years ago, we try never to forget that medicine is for people, people just like Ms. West, I might add.

Merck is solving its Y2K problem in order to ensure that we can continue to discover, develop, manufacture and distribute medicines that treat important human diseases. Our paramount goal is to ensure the continuity of the supply of medicines to our patients. At Merck we are doing so by following a simple strategy.

First, we have inventoried all computer systems, applications and devices with embedded microprocessors. Second, we have assessed each of these systems to determine whether it includes any date processing and whether its correct operation is of serious concern to our business. As an example of a system where we are less concerned about a possible Y2K bug, consider a program that reports monthly sales and organizes the columns of the report in chronological order. While we prefer to have the report continue to show the most recent results from right to left, if the Y2k were to merely cause the columns to print in a different order, this would only be a minor concern to us. We are deferring the repair of that kind of bug to the final stages of the Y2K project.

Third, we have developed a compliance strategy for each system. Fourth, we are executing that strategy for the many thousands of systems in our inventory. This is obviously a daunting task because of its magnitude and its geographic diversity. We have to deal with systems in the many hundreds of Merck locations worldwide.

The fifth and final step is to thoroughly test all of our systems. Our attitude is to trust no one but ourselves. If a system vendor tells us that their application is Y2K compliant, we will insist on testing it ourselves or at least auditing in detail the test results provided by the vendor. We have already found instances of applications certified compliant by the vendor that, in fact, did not pass our test initially.

As you can imagine, Merck's Y2K project is a very significant effort. We began reasonably early in 1996. There are now in excess of several hundred people involved. We are spending many tens of millions of dollars to plan, execute, and manage this work. Our goal has been to achieve Y2K compliance by the end of this year, thus allowing all of a 1999 for dealing with the inevitable glitches and inconsistencies among systems.

However, Mr. Chairman, fixing our internal systems is only part of the problem. Merck just as any global company works with many thousands of business partners, suppliers, customers, and government agencies. Our ability to continue our company's operations successfully in January 2000 depends just as much as on the Y2K programs of these companies and agencies as on our own internal systems. Hence, we have organized two other major sets of activity.

First, each business area is examining its business partners to assess its Y2K risk. If the proper operation of that entity's systems is essential for Merck's operations, we are both working with that entity to better understand its Y2K remediation plans and also developing internal contingency plans just in case that entity that fails to achieve Y2K compliance on time.

Second, we are working with the Vital Signs 2000 Project, which is a health system-wide effort organized by the Odin Group to gather important information about the Y2K compliance of the entire health care industry in which we participate. The Vital Signs 2000 team has developed a survey instrument for the five groups of entities comprising the health care industry: payers, providers, suppliers, distributors and government agencies. By understanding the cross-industry processes and their Y2K vulnerabilities, we together with the rest of the industry can develop the detailed contingency plans that can assure the continuity of high quality patient care.

What about the broader American pharmaceutical industry? While I obviously cannot testify about the detailed plans and projects of Merck's competitors, I have had the opportunity to discuss the Y2K problem with my colleagues in other pharmaceutical companies. These companies have all followed a methodology similar to Merck's and are applying the level of resources needed to deal with the problem. They have also recognized the broader issues of the readiness of business partners and are developing appropriate contingency plans.

Let me close with some broader context. I read periodically that companies and agencies are now just waking up to the severity of the problem—we have heard about that this morning. Worse, I still read and hear about entities that still do not believe that there is a serious problem. They may be right in their local situation but only an organized testing program will allow them to be sure. So I do worry about what will happen as the clock strikes midnight on December 31, 1999.

Again, I thank the committee for the opportunity to be here today and look forward to your questions.

[The prepared statement of Dr. Popper can be found in the appendix.]

Chairman BENNETT. Thank you very much. Mr. Streck.

STATEMENT OF RONALD J. STRECK, PRESIDENT AND CEO, NATIONAL WHOLESALE DRUGGISTS' ASSOCIATION

Mr. STRECK. Thank you, Chairman Bennett. The National Wholesale Druggists' Association, or NWDA, appreciates the invitation to testify today before the committee about the applications of Y2K. And I ask my written statement be entered into the record.

Chairman BENNETT. Without objection.

Mr. STRECK. NWDA is the national trade association representing distributors of pharmaceutical and related health care products. Our active member companies operate 215 distribution centers throughout the country that service every State, the District of Columbia, and U.S. territories. NWDA's active members provide distribution services to over 130,000 pharmacy outlets in the country including 21,000 independent pharmacies, 18,000 chain pharmacies, 7,500 hospital pharmacies, 220 mail order pharmacies, 7,000 food stores, 5,000 mass merchandisers, 4,000 long-term care and home health care facilities, 56,000 clinics and 1,000 HMO's.

Our most recent data indicates NWDA member wholesale distributors on average obtain products from over 750 manufacturer suppliers. Typically, a single wholesale distribution center stocks an average of 24,000 items and will process over 13,000 order lines per day. Virtually, all orders placed by pharmacy customers to their wholesale distributors are transmitted electronically and more and more electronic picking devices are used to fill these orders.

To service an increasingly demanding and integrated health care market, practically all wholesalers provide daily deliveries with a growing number of wholesalers providing twice a day deliveries to their customers. However, today's wholesalers do so much more than just deliver product in a timely manner. Some of the value added services NWDA members provide to their customers include marketing and advertising support, product sourcing programs and special handling services.

Other services provided that are especially relevant to the Y2K discussion are the computer and information programs that include third party claims processing and receivable services, inventory management, pharmacy computer systems for dispensing and care, and point of sale systems.

Wholesalers have been innovators and leaders in information technology. They continue to use information technology to integrate suppliers and customers. These programs and systems rely on automation, connectivity, information systems, electronic linkages, and network building that allow for the prompt and efficient delivery of lifesaving health care products.

Our members have been methodologically working to ensure their systems and those of their customers are compliant. You will hear more about exactly what wholesalers have been doing from Keith Mallonee of the McKesson Corp. in just a few minutes. Based on a number of suppliers, customers and orders, it does not take long to speculate on what would happen if there were an interruption of an electronic transfer of information. Many of these transmissions are reliant on commercial and government telecommunication networks, systems over which the pharmaceutical industry has no control.

NWDA and its members need to know that these vital communication networks are Y2K compliant and ready to support the delivery of health care services to the patient. This constant electronic transfer of information is the reason I am here today. As we have developed our association's web page, NWDA has devoted a separate section just for dissemination of general Y2K information. We endorse the notion of common solutions for common process problems and we are ready to move ahead with an industry clearinghouse for Y2K technical fixes that would allow drug wholesale trading partners to freely share such technical information.

We have been reluctant to proceed with this project due to liability and antitrust concerns. However, with the passage of the Year 2000 Information Readiness Disclosure Act, S. 2392, we understand that we will now be able to move ahead. We commend Congress for its approval of this important legislation and urge the president to move swiftly to sign the bill into law.

We are greatly concerned that Federal, State, and local governments are quickly running out of time to adequately test and correct all public service and infrastructure systems. It is disturbing to read reports from Congress and the GAO indicating that there are serious concerns, that many Federal agencies will just not be ready. The July 1998 report by the GAO entitled Year 2000 Computing Crisis concluded that quote "federal agencies and state governments suggest that the full extent of the managerial and operational challenges posed by the heavy reliance on others for data needed to sustain government activity is not yet known."

Congressman Steve Horn in his role as chairman of the House Subcommittee on Government Management, Information and Technology, has issued another report card on Federal agencies with HCFA once again receiving an F grade. We fear that Federal and State government agencies will not survive the changeover to Year 2000 without interruptions in health care reimbursements. Government reimbursement is only one area that could disrupt the flow of life sustaining prescription drugs to patients. Even if all parts of the prescription drug supply chain are compliant and ready, if there are failures in other links, it would be irrelevant that we are ready. We need assurances that government agencies will be Y2K ready so they can seamlessly carry out their important functions.

Wholesalers are making contingency plans to make sure that there is not a disruption in the availability of product. I want to emphasize that wholesalers are just one link in the chain. If the government agencies that play such a vital role in the health care system are not going to be Y2K compliant, contingency plans must quickly be completed and this information passed on to the public. How a business or industry develops its own backup plan depends on what government services will be available.

NWDA and our member companies stand ready to work with government at all levels to address these issues to ensure that life-saving medicines continue to get to those who need them when they need them. Time is of the essence, and I thank the committee for holding this hearing today to address this momentous issue.

[The prepared statement of Mr. Streck can be found in the appendix.]

Chairman BENNETT. Thank you. The buzzer has just gone off. There is another vote on the Senate floor. This time I think I will go immediately and come back instead of run the clock the other way. Mr. Mallonee, I apologize for mispronouncing your name. We will hear from you as soon as we come back. The committee will stand in recess.

[Recess.]

Chairman BENNETT. The committee will come to order. Mr. Mallonee, thank you for your patience. We will now hear from you.

STATEMENT OF KEITH MALLONEE, VICE PRESIDENT, SYSTEMS DEVELOPMENT, McKESSON CORP.

Mr. MALLONEE. Mr. Chairman, thank you for inviting McKesson to participate today. I know you are all busy so I will keep my remarks to about 3 minutes. My name is Keith Mallonee. I am vice president of Systems Development at McKesson. McKesson is the largest distributor of pharmaceuticals, health care products, medical and surgical supplies in the United States with over $20 billion in annual revenue. We serve customers in all 50 States through a network, a national network of distribution centers.

Our customers include independent pharmacies, hospitals, drug chain stores, food stores, clinics, nursing homes. We view the Year 2000 as a critical business issue at McKesson. We are in the health care industry. We understand the importance in ensuring that a critical and potentially lifesaving product gets into the hands of our customers on time. We are also heavily involved in electronic commerce. On a daily basis, we receive over 60,000 orders from our customers. We will fill over a million and a half order lines from our distribution centers. Over 99 percent of those orders come into us electronically.

So we are approaching Year 2000 at McKesson like we approach any major business issue or initiative and that is with a dedicated team of personnel, resources, dollars, and senior management involvement and oversight. We began the project, the Year 2000 product at McKesson, in 1996. We established a central Year 2000 project office for all of McKesson, which I head. It is my full-time job; it is my only job. It has been that way for 2 years and it will be that way for the next 18 months at least.

And we did the right steps, as you have heard before. We did the assessment. We inventoried our systems. We identified our key business processes. We developed detailed project plans, and then we sort of divided the Year 2000 project into what I call manageable chunks of work. We now have over 30 active Year 2000 project teams at McKesson. The majority of our systems have already been made compliant and we are in the final stages of taking care of the remaining software and hardware.

We intend to devote next year to intensive integrated testing, and that testing will include customers and suppliers. In addition, we have instituted a very rigorous project control methodology at McKesson for Year 2000 with regular review meetings with senior management that goes right up to the board of directors. While we are pleased with the progress that McKesson is making, we understand we are heavily interdependent with other industries, industries such as telecommunications, electric utilities, and transportation. We do need for them to be ready as well so that we can get product to our customer.

However, we are developing contingency plans. We are developing plans that will ensure that we can get product to our customers in the event that there is a disruption in business due to Year 2000. McKesson has been in business since 1833. During that time, we have faced numerous challenges in getting product to our customer. Hurricane Georges is a recent example of that situation for us. One of our distribution centers was closed because of the hurricane. But we have in place a backup system among our distribution centers. So we were able to reroute those orders from that distribution center to other distribution centers to get the product to our customers. That is the sort of contingency planning we will leverage as we go forward.

Year 2000 is a serious issue and it needs to be taken seriously and McKesson does. We think we know what we need to do. We have got the steps in place necessary to get it done and to achieve what we consider our primary objective in all this which really is no impact, no disruption to the customer. I would like to thank again the committee for inviting McKesson to participate in having discussions on this vital issue. Thank you.

[The prepared statement of Mr. Mallonee can be found in the appendix.]

Chairman BENNETT. Thank you very much. Mr. Carbray, you get to be the cleanup hitter.

STATEMENT OF RICHARD T. CARBRAY, Jr., GENERAL MANAGER, PELTON'S PHARMACY AND HOME HEALTH CENTERS

Mr. CARBRAY. I would like to commend whoever put this lineup together because as you can see you have got a manufacturer down to wholesalers to the end product, the dispensers of the medication. Good morning, Mr. Chairman. My name is Rick Carbray and I am representing actually three groups this morning. I am representing the American Pharmaceutical Association as well as the Connecticut Pharmacists Association and individually as a small business in Connecticut of three pharmacies in the central part of Connecticut.

And basically what I would like to talk about today is how it affects us pharmacists at the local level. You have heard some comments certainly from the manufacturers. McKesson is a wholesaler for our company, a very fine wholesaler, and we have done some due diligence with a lot of our companies to ask them if they are ready for this problem, and McKesson has responded very favorably. So we feel fairly confident and in talking to Ms. West regarding her testimony and how this might affect us and her as far as delivery of medications. I feel more confident today now talking strictly to McKesson and to the NDWA and to Merck that we do have in the pharmaceutical industry many of these situations readily taken care of.

What I do see, though, as far as a problem for some of us in the pharmacy industry is some of our systems where we in-house have already worked to get this compliance done. There are some systems, not necessarily related to the dispensing of a prescription which is obviously our most important function, those systems I can honestly say to you right now from our vendors, they are saying that they will be compliant. We have checked our pharmacy system as of last month and we were able to fill a prescription dated February 1, 1999 with a refill date of 2/1/00. So that prescription would have gone through that computer so we feel confident there.

We also are very involved in the whole home health area and obviously have concerns with those computers because now we also are tracking besides record keeping for pharmacy patients and medications and drug interactions, we are also tracking medical equipment and trying to do inventory control and billing. So we are looking to get compliance from those computer vendors also. An interesting situation that has just developed for us—it is more from a business standpoint, maybe not quite as much from the pharmaceutical standpoint—is our point of sale computer for our registers.

If we fill the prescriptions and we cannot collect for those prescriptions, obviously we will not be in business very long. Currently we have a vendor, a software vendor, who has provided us with a point of sale system who is going out of business, and it is interesting to note that they are going out of business because of the Year 2000 problem. They have decided that it is too cost prohibitive to address that problem as a company for their customers and they are going to get out of that part of the business. So we have roughly a $100,000 piece of equipment that is going to be relegated to some hardware very shortly.

We are in the process of working with other software vendors to hopefully assure us that we can upgrade that system to the tune of probably $40 to $50,000 in expense to become compliant. So again the pressures of a small business trying to stay viable and having to spend that kind of money.

In summary, again I feel fairly confident in the pharmaceutical end. Our big brothers have come to the table and I am very confident that we will continue to be able to deliver the products. If I can just comment, Ms. West and I talked about having medication available. A suggestion possibly to avoid some of the over stockpiling on a huge basis which I could see happening if a scare like this were to come out, pharmacists have generally been able to take care of individual clients with extra amounts of medication at our expense inventorying those medications and keeping them on hand to ensure that those patients that critically need lifesaving medication can have them. So as a general rule, I do not think we should go towards across-the-board overstocking or oversupplying but try to focus on those critical areas and help patients like Ms. West have that medication available. And with this group here, I think you have a group that is committed to doing that. Thank you.

[The prepared statement of Mr. Carbray can be found in the appendix.]

Chairman BENNETT. So if I understand what you are saying about the overstocking, you are saying that at the pharmacy level, you identify critical substances and have an adequate supply of that instead of having to have each individual patient have an unusual supply?

Mr. CARBRAY. Correct. We can identify groups of patients through our system and whether it be an AIDS patient or be a kidney transplant patient to make sure that we have plenty of supply on hand for that particular group. If it happens to be a kidney transplant patient as opposed to—and it can be specific to a patient also certainly. You may only have one kidney transplant patient that needs that medication so we would ensure that that medication is in ample supply although to be honest with you in most cases our wholesalers have an adequate supply.

I think what we are trying to avoid is a scare that forces the supply to change drastically and that people get an excess supply who do not necessarily need that excess supply and I think that could happen.

Chairman BENNETT. Dr. Popper, do you want to comment on this issue? I know pharmaceutical companies are concerned about the stockpiling challenge. One of the reasons for this hearing is to deal with what makes the most sense for consumers like Ms. West.

Dr. POPPER. Yes, I concur with the last comment that just stockpiling out of almost a panic situation is likely to create more harm than good, that it really distorts our ability to distribute product. Our position at Merck, actually even upstream of us, the companies that we get our raw materials from, the supply chain is very well engineered today and it is based on a certain expectation in terms of what supply is necessary in the marketplace and that ripples all the way back through the chain. If supply were to double or triple in the short-term, that kind of disruption to the supply chain could really, as I say, do more harm than good.

What I think we need to do is study the problem a little more. As I mentioned in the testimony, the Vital Signs 2000 survey will give us some good data on where we may see sensitivities in the supply chain and where we may see some risk. And I think on more of a rifle shot approach, we can understand where we want to take steps. So whether it is in certain cases at the local pharmacy, in certain cases at the distributors, in certain cases at our warehouses, we can make sure that we have the situation covered, but rather than take an across-the-board solution, which could be counterproductive, I think we need to work from facts which we have to gather over these next couple of months and then work out a plan that may entail some government help to make sure that we can get the cooperation together.

This now moves us perhaps away from the standard marketplace forces and I do not know where that may lead quite frankly. I just want to make sure that we do is based on a real analysis of data as opposed to just fear and panic.

Chairman BENNETT. One of the functions of this committee is to see to it that accurate information about all aspects of Y2K replaces some of the myths that are out there and the myths go all the way from the article in Time magazine that was headlined “Apocalypse Not” that basically said there is no problem to the folks that are digging up their backyards and putting in propane tanks because they assume they will not have any power for 5 years. And the best way to deal with both of those extremes of misinformation is hearings like this and witnesses like you that can give us that detail.

Mr. Popper or Dr. Popper, Merck & Co. is probably about as international as an American company is going to get, both in terms of your supply chain coming in and your distribution chain going out. I assume you sat here and listened to the Gartner Group presentation. Do you have any reactions or comments on Gartner’s view of what is going to happen around the world?

Dr. POPPER. From a Merck perspective, we continually review the risks on a worldwide basis. In fact, last week I spent 2 days with my senior staff devoted to yet another exhaustive review of all of our Y2K programs including the business continuity planning. And we have pushed down into each of the geographies beyond the United States, Europe, Mideast, Africa, Far East, Asia, and each of the countries is engaging in a similar activity.

So we are looking at the supply chain within each country and at our customer base in each country, the distribution chains, and doing what we need to in terms of contingency planning. So from a strictly health care perspective, we think we are engaged in the right level of planning to deal with the problem.

What I cannot really comment on is whether there will be systematic failures in some countries of the infrastructure. Our planning assumption is that the more advanced countries that are more heavily computerized are typically further along in the planning stage. I think Gartner had some countries that I want to go back and double-check on because it sort of goes counter to that assumption, and then some of the countries where they are less developed there is actually less reliance on that infrastructure and that I think mitigates the risk. So that has been our approach to it and as I say, we will look at their data very carefully and make sure that there are no surprises there that we have to worry about.

Chairman BENNETT. Well, let me put on my CEO hat that I wore and say, all right, we are sitting in my corner office now and we are 6 months away from New Year’s Eve in 1999. I am saying to you, OK, doctor, it looks like Country X—I will not fill in the name here lest anybody get excited—is going to have insoluble Y2K problems. You have been developing plans and I assume that means we start buying whatever someplace else. Is that, in fact, the kind of conversation you are going to have with your CEO? If it is, do you have a list of someplace else?

Dr. POPPER. On the supply side, we have that covered on a worldwide basis. We have looked at every single supplier. We have categorized them in terms of criticality of the supply, uniqueness of the supply, and are dealing with that. Most of our production is focused in a small number of countries. We have 30 plants worldwide including I think about 8 in the United States. So it is on the order of 20, 25 plants outside of the United States and those are situated in places where we are pretty confident that the infrastructure will survive and we will not have any problem with that. So I think the bigger risk in the smaller countries is on our ability to supply downstream and the ability to distribute through the network then.

Chairman BENNETT. I see. You are concerned more about your customer chain that your supply chain?

Dr. POPPER. Exactly.

Chairman BENNETT. Well, I am coming back to the theme that I mentioned when I was talking to the small business group. The more this unfolds, the more convinced I am that we are going to see a flight to quality with corresponding dislocations on the part of marginal producers, marginal companies, marginal countries. Every one of these hearings teaches me something. I have now sat through I do not know how many with the combination in this committee and the subcommittee that I chair on banking for financial services and technology. I guess we are approaching 20 hearings total; are we not? 18. All right. Well, in Washington-speak, that is 20. And I learn something from each one.

Sometimes I am reassured by what I learn. There are some things we have heard today that are quite reassuring. Sometimes I am more frightened by what I learn and there are some things we have learned today that are frightening. But I recently have come to the conclusion that as a result of Y2K, we are going to see significant shifts in where people go for materials, where people go for markets, and it will produce some very challenging social problems all over the world. Then those countries and companies that survive and thrive as a result of the long-range planning that they have done will be called upon to provide aid and assistance in those parts of the world where challenges exist. I think the social impact of this is beyond anything we had previously thought it might be.

CLOSING REMARKS

I would like to thank today's witnesses for their valuable contribution to our growing understanding of Year 2000 issues.

Let me take just a moment before we close to quickly summarize the committee's activities this session. In the 6 months of our existence, we have accomplished a great deal. The committee has held nine hearings on critical infrastructure and industry sectors including energy utilities, health care, telecommunications, transportation, financial institutions, general government, and today—general business. And against impossible odds, we also managed a bipartisan effort that passed the Year 2000 Information Disclosure Act (S. 2392). In addition, our CRASH protection legislation (S. 1518) forced the SEC to require meaningful Y2K corporate disclosure to shareholders. This disclosure will help maintain faith in our markets, and ensure the availability of accurate Y2K information from publicly traded companies.

Raising awareness, highlighting potential Y2K problems and prompting action on Y2K have been of central concern to the committee. We have maintained a bipartisan approach to the committee's activities, and worked closely with the President's Council on Year 2000 Conversion, as well as numerous industry groups. All of us have a common goal—to minimize the impact of this potentially devastating problem.

While awareness of the Year 2000 problem is growing, we still have much work to do. Our research indicates that many organizations critical to our safety and well being are not fully engaged in solving the problem. For example, over 90 percent of the doctor's offices and 50 percent of the small and medium sized businesses have yet to address the problem. Like ostriches, they are burying their heads in the sand—unwilling to believe that the problem is real, or content to think that someone else will solve it. This complacency is very dangerous. While larger firms have to some extent grasped how a Y2K failure could severely impact their future, smaller firms seem to be more focused on their immediate problems.

The findings of our committee do not just indicate a division between small and large organizations. First, nearly all affected industries and organizations started too late. As a result, most organizations must exercise triage—focusing on what is critical to sustain the life of the enterprise as opposed to finding long-term solutions. Second, there are still no overall assessments of infrastructure or industry sectors. Consequently, we still cannot answer the fundamental questions that everyone is asking—How bad will it be? Which systems are most at risk? And, what should I do personally to be prepared? Third, this is a global problem. That means that any business, government agency, or other organization that has international operations must pay attention to the affects of Y2K in other countries. If the United States is the leader in addressing the Y2K problem, and the situation is as gloomy as it is here, then the prospects for the rest of the world are positively frightening. Fourth, if it becomes increasingly evident next year that we cannot finish the job, contingency planning will become even more criticalessential. Finally, the fear of legal liability, while it has stirred some to action, has discouraged organizations from openly sharing information. As a result, those trying to address the problem have found themselves inventing their version of the wheel instead of collaborating with their industry counterparts.

Just last Thursday the Congress passed the Year 2000 Information Disclosure Act. Having received the administration's proposal with only 25 legislative days remaining in this Congress, there were those that doubted our ability to pass this bill. It was a pleasure to prove them wrong! We are convinced that the Year 2000 Information Disclosure Act will encourage the exchange of Y2K information and, thus, give organizations invaluable access to information that they would not otherwise have had. This information should save companies precious time in their Y2K remediation efforts, and greatly aid those companies who are grossly behind on their Y2K planning.

While we are out of session and back in our home States, we will continue to work closely with our staff investigating potential Year 2000 problems, pushing for assessments of our critical infrastructures and researching the implications of international Y2K failures. I look with guarded optimism toward 1999. We all must be relentless in our pursuit of the Y2K bug. We end this congressional session hoping for the best, but preparing for the worst.

Thank you all very much. Again, I apologize for the somewhat disjointed fashion of this particular hearing, but it has been very useful and I am particularly grateful to those of you who are willing to come forward and share your information. The committee is adjourned.

[Whereupon, at 12:38 p.m., the committee adjourned.]

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

Prepared Statement of Chairman Robert F. Bennett

Today marks the Committee's ninth and final hearing this year. In all of our hearings we have strived to increase awareness, disseminate reliable preparedness information, and help facilitate solutions. This Committee has spent the last 6 months trying to raise public awareness of this oncoming challenge. Despite our best efforts, recent polls tell us that only 30 percent of our fellow Americans have heard about the year 2000 problem. Only 450 days stand between us and the new century. Our work—the work of everyone participating in this hearing today—becomes more urgent with each passing day.

General business—the subject of today's hearing—is a term that encompasses the spectrum of American commerce ranging from over 5 million small firms at one end of the spectrum to global corporations at the other end. All of these companies face Year 2000 challenges—from the PC's and networks automating their offices to their dependence on credit card transactions, just-in-time inventory supply systems, Electronic Data Interchange (EDI) transactions, and other technologies. One of today's witnesses warns that over 700,000 small firms are at risk of either closing their doors or being severely crippled by Y2K problems.

Global corporations face complex problems because of their dependence on thousands of suppliers, distributors, and customers, both domestically and internationally. They must be concerned not only about the Y2K readiness of these business partners, but the infrastructure of the countries where they reside. Today, the Gartner Group is releasing some alarming new research data which shows that 66 percent of the companies in critical industries such as healthcare and food processing will likely experience at least one mission critical systems failure. In addition, 50 percent of the companies in critical trading partner countries such as Germany, Japan, Saudi Arabia, and Venezuela will experience similar failures. If these predictions are correct, Y2K could deliver a devastating blow to an already troubled global economy.

I would like to relay an example that shows how even the smallest of businesses are completely reliant on technology, and, thus, highly susceptible to Y2K risks. Recently, an acquaintance cracked his car windshield. He replaced it by calling his insurance company whose national computer directory located a local glass installer for him. This two-employee business received an electronic purchase order from the insurance company authorizing the replacement of the windshield. The glass installer in turn compared the year and model number of the car to his database in order to place the appropriate EDI purchase with a large supplier of windshields. When the windshield was installed on site at my friend's home, less than 24 hours later, my friend marveled at the efficiency of the process. The small businessman replied that his company, like most others is striving to improve service and reduce costs.

For exactly that reason, small businesses, like the one in this example, depend heavily on EDI to eliminate paperwork and reduce transaction time. Electronic purchase orders, inventory control and payments processing are greatly facilitated by EDI. This story also highlights the critical role that just-in-time inventories play in many small businesses. Unlike their large, corporate counterparts, small businesses cannot afford to store and maintain the thousands of non-standard parts and supplies. While EDI makes just-in-time inventories possible, the use of this and other technologies heightens our concern about the impact of Y2K, and, thus, the viability of America's businesses. One recent study estimates that over 600,000 firms are at risk of either close their doors or be severely crippled by Y2K problems.

This micro example of modern commerce demonstrates not only the central role that technology plays in today's commercial world, but also the mutual dependency of large and small businesses. To small businesses, we offer this caution from the editor of CIO magazine, a witness at our recent Telecommunications hearing. He stated, "Large companies are starting to perform Y2K triage work with their partners connected in massive EDI or other telecommunications networks where they are abandoning entirely those companies not essential to their critical business processes that may not be Y2K compliant." This is a real and present danger that small firms must address. When the first EDI transaction is placed on January 3rd of the year 2000 the small business on the receiving end may only have one opportunity to respond. If it fails to do so, the competitive environment will quickly force that small firm out of business.

As we examine each industry in detail we are discovering that inter-connectivity among businesses is one of the most difficult Y2K issues to address. You can be ready for the Year 2000, but your key business partners may not. In addition, any break in the electronic link between you and your partners both here or abroad could be equally disruptive. Companies must assess these issues and find alternative partners if they are to remain viable after the Year 2000.

The frustration that Vice Chairman Dodd and I share along with the other members of this Special Committee, is that many of those who are dragging their feet on the Y2K issue defend their lack of activity on the perception that we lack adequate information to justify serious action. Perhaps 6 months ago we were flying blindly into the year 2000, but thanks to the many publicly-spirited Americans who have testified before this Committee, patterns are emerging. We do not need absolute, 100 percent certain evidence for us to recognize that we have a serious Y2K problem any more than a citizen of Key West or Mobile needed the National Weather Service to tell them that they were in the middle of a hurricane. The Weather Service did, however, provide an absolutely invaluable function by warning of the oncoming danger. Like the Weather Service, this Committee cannot provide an absolute prediction of the future. We cannot know what will happen on January 1, 2000. We can, however, provide a real and useful warning for individuals and industries, and that, after all, is one of the most important aspects of our work.

Our hearing today is intended to be a catch-all for general business Y2K issues—from small businesses to global corporations. We have a panel to represent small business concerns, and a pharmaceutical industry panel to represent articulate the Y2K problems facing global corporations. We welcome today's witnesses and thank them in advance for their contribution to this extremely important issue.

Prepared Statement of Richard T. Carbray, Jr.

Good morning. Mr. Chairman and Members of the Committee, thank you for the opportunity to present the views of pharmacist caregivers across the country on the impact of the "Year Two Thousand" (Y2K) problem on the pharmacy profession and the patients we serve. I am Richard Carbray, a pharmacist, and I am speaking today on behalf of the American Pharmaceutical Association (APhA), the national professional society of pharmacists, and the Connecticut Pharmacists Association. This topic is important to me and my profession for one central reason: perhaps more than any other part of the health care industry, pharmacy is the most reliant on computers for nearly every component of day-to-day activity.

Pharmacists rely on computer technology to maintain patient drug therapy records, identify potential drug interactions, and provide clinical information about medication use. Computers are used to print out relevant patient information about prescription medications at the time of dispensing in community pharmacies, used to track drug therapy within the hospital and long-term care facility, and to submit claims for third party payment. Nearly every one of the more than two billion prescriptions dispensed in the United States is prepared with the assistance and support of a computer. Pharmacists will directly feel the impact of any failure in these systems due to the Y2K problem. The issue this Committee addresses today will have some relevance for nearly every one of the 118,000 pharmacies located in communities, hospitals, and home health clinics in the United States, including more than 40,000 retail pharmacies.

USE OF COMPUTERS IN PHARMACIES

Pharmacy is likely the most computerized segment of the health care industry, with an estimated 99 percent of prescriptions dispensed using computers. Let me quantify this for you: in 1995, prescriptions filled in retail, long term care and mail service pharmacies totaled more than 2.3 billion. This does not include prescription medications dispensed in hospitals and other settings. With advancements in medication therapy and increasing reliance on these agents, these numbers will only increase and increase the use of computers in these settings. Most pharmacies use computers for virtually every aspect of day-to-day operation. For example, in any given pharmacy there may be different systems to track sales and inventory and maintain patient profiles, check for drug interactions, track prescription refills and maintain patient records.

In addition to this use within the pharmacy, on-line, real-time transmission of claims for third-party coverage of prescription drugs is a normal component of pharmacy practice. The claim for third party coverage of the prescription is transmitted to a claims processor, such as a State Medicaid agency, for on-line, real-time review of the prescription to confirm eligibility of the patient for coverage and conduct some drug utilization review activities. In 1996, more than one billion prescription claims were processed in this manner, supported by the industry telecommunication standard as developed by the National Council for Prescription Drug Programs.

CHALLENGES WITH YEAR 2000 COMPLIANCE

Like many other health professions, pharmacists rely on outside software vendors to develop and maintain the various operating systems used by the pharmacy. Many vendors have indicated that their products are Year 2000 compliant, but what assurance does the pharmacist have? This uncertainty, likely typical of many approaching this daunting problem, places the pharmacist in a somewhat vulnerable position—he or she must trust that the software is compliant, but will not know for sure until the first prescription is entered that could trigger a problem. An error in the in-store system or in the third-party processing system will likely stop progress on preparing that patient's medication, and likely cause delays for other patients. At a minimum, concern about these problems and dealing with them as they arise will distract these health care professionals from their core function—working with patients to make the best use of their medications—to focus on challenges with the systems designed to support that practice.

The problems for pharmacy will not wait for January 1, 2000, either. Many pharmacists will confirm or discover their challenges with Y2K compliance in early January of 1999. Let me explain. Most prescriptions for chronic medications, like a drug to control high cholesterol or blood pressure, are valid for one year. In entering a new prescription into the pharmacy operating system, an expiration date for the prescription is also entered. When Mrs. Smith brings in her prescriptions on Saturday January 2, 1999, I will know pretty quickly if the system is compliant. If it is not, the expiration date of January 2, 2000, will cause an error and reject the prescription.

This is not, however, the first time the profession of pharmacy has faced date-related challenges. In the early stages of computerization end expansion of clinical systems to support pharmacy practice, the inclusion of patient birth dates provided necessary information to confirm patient identity and focus clinical information provided to the pharmacist. Communicating the birth date of patients born in the late 1800's created a preview of the expiration date problem we expect. Obviously, a birth year reflected by "87" and interpreted as a birth year of 1987 will yield different clinical recommendations than the more accurate birth year: 1887. This problem was addressed at that time for the birth year, and we hope all Y2K problems will also be addressed. Pharmacists may have varying comfort levels that the systems have dealt with the problem before, but are concerned about the impact on other data fields, such as the expiration date.

EXTERNAL COMPUTER SYSTEMS

Beyond the operating systems within a pharmacy, pharmacists must also rely on the compliance efforts of a number of systems involved in processing claims and third party payments. To secure third party payment for prescription medications, the information is transmitted from the pharmacy system to the system of the third party payer—often through a "switch" to direct the information. Some of this information stays within the originating state, for processing by the State Medicaid program, for example, but other information may pass through a company located in a city hundreds of miles away, and then onto its final destination in yet another system located in yet another state. The claim is then processed at the remote location—verifying patient eligibility, coverage for the specific product, and some utilization review procedures conducted. Approval for payment and/or relevant clinical or administrative information is then transmitted back to the pharmacy.

This process occurs on-line, in real-time at the pharmacy—literally while the patient is waiting for their prescription. Any glitches in the system from the third party processors or the switch company will create problems in my pharmacy—and delays for my patients. Again, this diverts my attention from clinical activities and patient education to trying to release the prescription and verify coverage and payment. I communicate with a number of third party processors every day, and must rely on those companies to ensure Y2K compliance.

In this overview, I have not even begun to address the additional challenges created in other areas of my pharmacy outside of the prescription dispensing area. Similar to other small businesses, I must also be concerned about challenges with credit card processing, inventory control systems, and the myriad of other computers with which I work every day.

CONCLUSION

The impact of Year 2000 compliance will be felt in many areas of pharmacy practice—the retail side with the cash registers and inventory programs, in the home health care and durable medical equipment area, and for prescription processing and record-keeping. Beyond the challenges in one's own pharmacy, there is interaction with other computers constantly—and pharmacists must trust that those systems will be compliant.

Pharmacy will experience the impact of glitches in Year 2000 compliance sooner than other health care providers, with January 1 of 1999 the first date for potential problems. We are working to alert pharmacists to check on the compliance of their systems—and take action to avoid problems. Thank you for conducting this hearing, and for listening to the concerns of the nation's pharmacists.

RESPONSES OF RICHARD T. CARBRAY, JR. TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. The monitoring of expiration dates is an important safety control in the pharmaceutical business. What are the Y2K vulnerabilities of your business in the area of inventory control?

Answer. The absence or delay in providing expiration dates on drug products would certainly affect inventory levels in that drug products with slower movement would require additional re-order processing to ensure full potency. Although this would not necessarily require more amounts of drug product in stock at one time, the frequency of ordering would certainly increase.

Question 2. Drug interaction information and patient drug sensitivity information are an important part of pharmaceutical records. What is the potential impact of Y2K in this area?

Answer. If the clinical information regarding patient drug therapy is restricted or unavailable, there will be significant impact on the pharmacists' ability to not only dispense medication, but also to consult with patients as to the proper use of that medication, particularly if potential drug interactions exist. If these systems are not in place it would be virtually impossible to provide drug products to a patient in a timely and precise manner. The checks and balances of the information available in the data base is critical to proper medication dispensing.

Question 3. What are the electronic data interchanges do you rely on for the receipt and transmittal of information in your business? What vulnerabilities do you see in this area?

Answer. Currently almost 65–70 percent of all prescriptions dispensed are covered under some form of insurance company (private, Medicare, Medicaid, HMO). Since 99 percent of the prescriptions filled are done through computer, pharmacies must rely on third party claims processors for on-line, real-time review of the prescriptions filled. In 1996 over 1 billion prescriptions were processed in this manner, supported by telecommunications systems. the vulnerability is that the pharmacist must trust that these vendors have complied with the Y2K requirements. The result of non-compliance leaves the pharmacist with no adjudication of the claim and the patient without the medication.

Question 4. As a customer, what are your main concerns regarding the Y2K readiness of pharmaceutical manufacturers?

Answer. The overall concern would be that manufacturers would not be able to supply pharmacies with the needed drug product for our patients. A huge potential for stockpiling by larger chains and mass merchandisers could cause a supply shortage and impact the ability of smaller pharmacies to get the needed products for their patients.

Question 5. What is your reliance on foreign produced pharmaceutical products? How does this reliance factor into your risk assessment related to your Y2K exposure?

Answer. Currently our company has a very small volume of foreign produced pharmaceutical products. However, there are some manufacturers who have foreign subsidiaries which could affect some product flow if a problem arose. Although we have some concern we will rely heavily on the U.S. manufacturers to ensure that product is available.

Question 6. We've heard earlier today that one effective way of reaching small businesses is through their trade associations. The web page for the American Pharmaceutical Association (APhA) states that APhA represents 50,000 pharmacists, pharmaceutical scientists, etc. However, we could not find any reference on this web site to Y2K or Millennium Bug. What can Congress or the government do to increase Y2K awareness and encourage greater outreach on the part of trade associations?

Answer. I think that trade associations are an excellent way of disseminating information regarding issues like the Y2K problem. I have received information from APhA on this issue and feel that they have been diligent in notifying members of this situation. Congress should continue to contact trade associations for their input on these issues. The associations in turn will filter down the information to its constituents. Requests from Congress to associations for individuals to present testimony certainly is valuable. The lines of communication must flow in both directions to be sure.

Prepared Statement of Senator Susan M. Collins

I wanted to first thank you Mr. Chairman for your continued leadership on this critical issue facing our nation. Over the past four months, this Committee has examined vital areas of our country's technology infrastructure.

We started in June with our utilities hearing, and since that time the Committee has focused on telecommunications, banking/finance, transportation, and emergency preparedness. But of all the hearings we have held, today's hearing, with its focus on Y2K's impact on business, and especially small business, might be our most important.

Our nation's 23 million small businesses create two out of every three new jobs, represent over 99 percent of all employers, and are responsible for more than half of the nation's technological innovation. In my home State of Maine, they are the backbone of our economy.

While we have received assurances of other industry sectors' preparedness for Y2K, there is great concern about small business. Many small businesses are having difficulty in determining how they will be affected by Y2K and what they should do about it. Many of them face not only technological but also financial challenges in becoming Y2K-compliant. Most of all, they need practical information about what to do.

The good news is that information resources are available for small businesses to assist them in figuring out what to do. In fact, I wanted to welcome two people who know how to help small businesses and are working every day to tackle the Y2K problem. First of all, I wanted to welcome Fred Hochberg, Deputy Administrator of the Small Business Administration, an organization I am very familiar with having served as its New England Administrator during the Bush Administration.

Mr. Hochberg joined Senator Snowe in Maine in August rolling out his agency's "Are You Y2K OK?" program, encouraging the small businesses in my State to identify potential Y2K problems, take action on them, and stay informed about new developments. This is an excellent outreach program, and I commend the SBA for its leadership role on Y2K.

I also wanted to welcome Rod Rodrigue from Maine. I had the opportunity to meet with Rod last month in my of floe and was impressed by the tremendous amount of knowledge and energy he brings to this issue. Thanks to his leadership, the Maine Manufacturing Extension Partnership has taken the initiative in reaching out to small businesses to help them cope with the Y2K challenge.

The Maine MEP uses a diagnostic software tool to assist businesses in identifying specific Y2K problem areas and then provides a road map for businesses to find further information in their Y2K remediation process, including links to SBA loans if necessary. Congress should take a very close look at this model program funded through the National Institute of Standards and Technology and the Department of Commerce.

Mr. Chairman, by their very definition, entrepreneurs are risk managers. In the years that I have been working with small businesses, I am aware of countless experiences where the entrepreneurial spirit has propelled business owners to overcome major obstacles to succeed.

While we will hear about reasons for concern about small businesses and Y2K in today's hearing, we should not lose sight of their ability to adapt. Coupled with tools and resources from organizations like the SBA and Maine MEP, it is my expectation that small businesses will succeed in solving their Y2K problem. I look forward to learning more from today's witnesses about how the federal government can assist in achieving this goal.

PREPARED STATEMENT OF WILLIAM J. DENNIS, JR.

Thank you, Mr. Chairman, for the opportunity to present evidence on the preparedness of small business owners for the Y2K problem. The bulk of my testimony consists of the attached report. It outlines and quantifies the status of small business owner preparedness as of late April. These data will be updated later this month meaning that new numbers will be available around the first of December, perhaps sooner.

My judgement is that the late October/early November update will be more encouraging than last spring's baseline. A year and one-half, i.e., the time between the baseline survey and January 1, 2000, can be an eternity to a small business owner. Immediate problems are usually those tackled first. As we near the critical date, I anticipate Y2K will begin to move up the priority scale. However, this is speculation based on experience rather than the statistical evidence NFIB will soon be collecting again.

The critical finding from the April survey is that just over 80 percent of small employers in the United States are exposed to a possible Y2K problem through their computers. A non-mutually exclusive 35 percent believe that they have devices with embedded chips. Despite this extensive exposure, a majority of small business owners plan no action.

Think of the small employer population as divided into fifths. One-fifth has taken action or is in the processing of taking action on Y2K. One-fifth plans to take action prior to January 1, 2000, but has not yet done so. Two-fifths have not taken action and do not plan to do so. And, the final fifth has not heard of Y2K.

At one extreme are the one in five small employers who do not need to take direct action. No equipment in their businesses exposes them. Their concern rests with others, e.g., their suppliers, their financial institutions, their utilities, etc. Joining them are another one in five who are in the process of resolving any problems they may have. The result is that about 40 percent of the population now appears to be clear of direct problems.

Should nothing change, approximately 330,000 businesses will inhabit the other extreme. They will have to shut down for all intents and purposes on January 1, 2000, and stay closed until their Y2K problem is fixed. These firms are exposed, would suffer an 85 percent or more loss of production or sales should their computers malfunction, and whose owners in April planned no action. The severity of the individual impact will depend the speed and the cost of rectifying the problems, and/or the costs of alternative production or sales systems. Small employers in this situation must understand, however, that the supply of people who can correct Y2K problems are limited and that on January 1, 2000, the demand for their services (and their fees) will be great leaving these business owners at the end of the line. I must emphasize that this is a worst case scenario. It means that serious malfunctions occur in all of the firms possessing the characteristics outlined above. That almost assuredly will not happen, but it clearly suggests the potential impacts are not trivial.

A majority of small businesses fall in the middle. They may be impacted and if they are, some damage will ensue. But, the damage will not cripple the operation. Still, this group, too, will require people who can solve Y2K problems. And, they too will have to wait in line and pay dearly to get them.

Aside from liability and an assumption that the credit markets don't suddenly "go into the tank," the Federal government's role toward small business should principally be one of the village nag. Washington should use its pulpit and encourage others to do so as well. Let me point out that the SBA's Office of Advocacy sponsored research (How Small Businesses Learn) in 1994 that outlines the most effective means for government to communicate with small business owners. I can find no evidence that anyone outside Advocacy and a handful of others have ever read the report. But it offers useful insights useful for the present situation.

"How Small Businesses Learn" documents that government isn't particularly credible with small business owners nor are it communications. However, industry-specific trade associations are and their literature is read. Moreover, industry-specific trade associations have some knowledge of the specific equipment used by businesses in the industry. Many of these groups can, therefore, identify and offer suggestions on embedded chip problems that those outside the industry almost certainly cannot. Suppliers and business associates are another source of credible information. Larger firms and financial institution are now often asking their customers about Y2K "compliance." The certain effect of these actions by business associates is to make small business owners increasingly aware of the problem and the seriousness with which their peers people take the problem.

The upshot is that government might do well to focus its pulpit activities on leaders of trade groups and larger businesses with large supplier networks. They reach deeply into the small business community are have notable credibility. While they do not reach everyone directly, they do reach a critical mass.

I would be remiss in failing to explicitly mention the contribution of the Wells Fargo Bank in the Y2K activities outlined. Wells Fargo has underwritten NFIB's small business Y2K surveys and has prepared a Y2K booklet for small business owners. Copies of the booklet are available for the committee and staff.

Small Business and the Y2K Problem

[William J. Dennis, Jr., NFIB Education Foundation, May 26, 1998]

Key Words:
—Automated Processes
—Computers
—Liability
—Microchips
—Size of Business
—Small Business
—Small Employer
—Timing/Dating Mechanism
—Urban/Rural
—Y2K (Year 2000) Problem

The Wells Fargo Bank sponsored the research on which this report is based.

1. INTRODUCTION

More than eight of 10 (82 percent) small businesses face direct exposure to a Year 2000 (Y2K) problem. Eighty-one (81 percent) of their owners say that they are aware of it. However, fewer than one in four (23 percent) consider Y2K a serious problem. This gap between exposure and perceived problem severity is not necessarily inconsistent. A timely, measured response to a looming problem is the optimal method of resolving difficulties. Yet, just 41 percent have taken action or plan to take action to address the potential Y2K problem. The resulting interval between exposure and plans to address the potential problem has adverse implications for small business owners. If the experts are correct about the consequences of Y2K and small business owners are not prepared, many could face significant repercussions that, at a minimum, will make their business lives uncomfortable.

2. MOST SMALL BUSINESSES EXPOSED TO Y2K

The Y2K problem is located in computers—hardware and software, timing/dating mechanisms, and various types of automated equipment. Not every computer in operation nor every piece of software, nor every timing/dating mechanism will yield a Y2K problem. However, it is not always possible to easily determine which devices contain the problem and which don't. The small business population that will be (or would be) impacted—in contrast to the potentially impacted or exposed population—is not obvious.

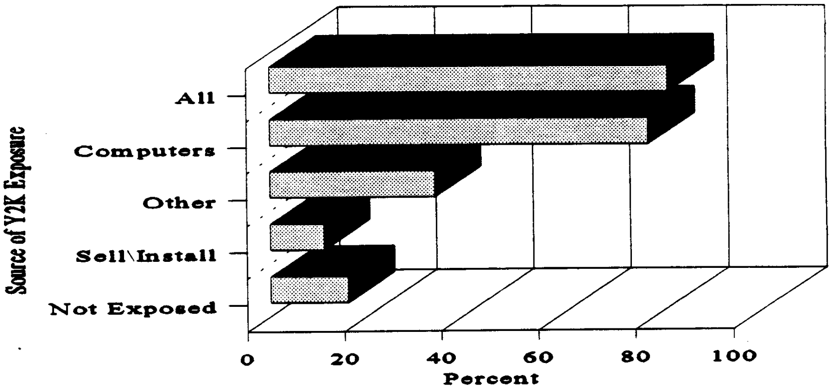
The same is true for the organizations with which a small business transacts its affairs. These business partners may be large or small, profit or non-profit, public or private. But since these entities face the same Y2K problem, and since it takes at least two to conduct a business transaction, the effect of Y2K on any individual business is a function of the individual business's problem as well as the problems of its partners.

2.1 Direct impacts

Eighty-two (82) percent of small business owners[1] are exposed directly to the Y2K problem. Exhibit 1 presents the sources of exposure. It includes the percent of small business owners who use at least one computer in their businesses (78 percent), the percent using other equipment or devices that might be impacted (34 percent), and the percentage selling, leasing, or installing equipment that could be affected (11 percent). These categories are not mutually exclusive. Exposure overlaps in many organizations. The "Not Exposed" category on Exhibit 1 quantifies the percentage of firms which appear to have no direct exposure. This 18 percent of firms possess none of the suspect equipment nor do they sell/lease/install any of it.

The large majority of small employers, an estimated 4¾ million, are exposed to the Y2K problem. Computers are the primary reason. Virtually every firm facing Y2K has an exposure through its computers. Other devices and equipment increase the total exposed by only four percentage points.[2] The final exposure category comes in those firms which sell devices and products that may contain the Y2K problem. These firms appear liable for their products and services, not just for replacement or repair, but for the damage a malfunctioning product might cause. Virtually all the firms in this category fall in at least one of the other two categories as well.

EXHIBIT 1.—PERCENT OF SMALL BUSINESSES WITH DIRECT Y2K EXPOSURE BY SOURCE OF EXPOSURE



Larger small firms are those most likely to be exposed. Businesses employing 25 or more people use computers almost universally. They are also more likely to possess other timing/dating devices (46 percent) and to sell, lease or install products with potential exposure (19 percent). Small business owners employing 1–4 people lie at the other extreme. Only 70 percent of this group use computers in their businesses, and their potential exposure in other ways is proportionately less as well. Still, 2¼ million of these small employers face a potential impact. The same phenomenon appears when substituting annual gross sales as the measure of size (Exhibit 2). About ⅔'s of those grossing less than $250,000 are exposed. Once revenues reach $500,000, everyone is exposed for all intents and purposes.

Exposed small businesses are also more likely to be located in metropolitan areas than in rural areas (Exhibit 2). Just, eight percent of firms in metropolitan areas (defined as city and surrounding suburbs with 500,000 or more) are without computers in their businesses compared to 37 percent in rural areas (defined as community of less than 5,000 or a rural area). The survey contains four geographic size measures. The frequency of computer use grows in every category as the resident population becomes larger.

Other demographic characteristics of the business and/or the owner show no relationship to the Y2K problem.

[1] The survey covers only those who employ other people. It does not include self-employed individuals who employ no others. The Y2K problem of the six million full-time self-employed without employees probably resembles that of the smallest employers, and is in addition to it.

[2] The other equipment and devices category presents definitional problems for those de signing the questionnaire as well as for respondents, and therefore is the response most likely to contain bias (though in which direction we do not know). The difficulty probably has little impact on the estimate of total firms exposed since computers make most firms exposed in any event. The difficulty arises in quantifying the nature of exposure.

EXHIBIT 2.—EXPOSED SMALL BUSINESSES BY ANNUAL GROSS SALES AND URBAN/RURAL DESIGNATION

Annual gross sales	Exposed to Y2K (percent)	Urban/Rural	Exposed to Y2K (percent)
<$250,000	67	Metropolitan (500,000+)	92
$250,000–$499,999	87	Large city (50,000–500,000)	86
$500,000–$999,999	96	Small city (5,000–49,999)	76
$1,000,000–$1,999,999	95	Rural (<5,000)	67
$2,000,000+	100	No answer	100
No Answer	96		
All Businesses	82	All businesses	82

2.1.1 Size of the direct impact

Exposure to a Y2K problem does not necessarily translate into serious problems. A piece of equipment lost for a day or two may be more of an inconvenience than a serious liability. Exposed small business owners on average estimate that one-quarter (24 percent) of their sales or production would be lost for the period that affected equipment or devices did not operate. That impact estimate is consistent across size and geographic area, with the production industries, i.e., construction and manufacturing, impacted marginally less than services. An affected business, grossing $750,000 annually, could expect to lose $3600 or 0.5 percent of sales directly if a Y2K problem took one week to resolve. Indirect losses, such as good-will, are more difficult to calculate, but would add to the total.

The impact estimates diverge wildly among firms. Seven percent would have to virtually shut down if, as forecast, these small business owners experience impacts at 91 to 100 percent of sales or production. Another eight percent gauge impacts between 71 and 90 percent. Those figures translate into over 330,000 businesses shut down and a slightly larger number crippled. But 330,000 is the worst case and assumes that everyone exposed is impacted. Everyone exposed will not be impacted as many in the group will take preventive measures and others will prove to have non-affected equipment. Yet, only one-quarter of the group who believe that their sales or production would be down by 71 percent or more if their systems malfunction have taken action though another 40 percent plan it. These latter figures are based on a very small n (n=52) and therefore must be used with considerable caution. But the numbers do suggest that far from all who attach significant dependence to their computer and automated systems are convinced that Y2K is worth addressing.

Forty (40) percent of the directly exposed owners estimate their sales or production would be impacted by less than one percent. This group will bear any impact of Y2K through the cost side only, at least initially. Handwork will substitute for computers or other automated processes. For example, payroll checks may have to be individually handwritten rather than produced automatically. Such substitution will add to costs. (The survey captured no data on the size of these costs, though they obviously could range substantially.) Added costs at some point must be passed on in the form of higher prices. Higher prices make affected businesses less competitive which can subsequently impact sales or production.

The unknown variable is the length of time impacted businesses will “be down.” Affected devices will malfunction 9/9/99 or 1/1/00. Unfortunately, everyone’s Y2K problem will occur at the same time. A limited number of people will be capable of detecting and fixing the conditions, at least the more serious ones. Demand for these experts will exceed supply. Their fees will rise sharply. Even then these experts may not be available for some time. The alternative is to have the owner or an employee do the work. The success of this latter strategy will vary enormously.

The more businesses impacted by the Y2K problem, the greater the number of small business owners who will face “down-time.” Small business owners, therefore, have an interest in having as many businesses as possible resolve their Y2K problems early.

2.1.2 Types of activities affected

Several business functions could be adversely affected by a Y2K malfunction. For example, 21 percent of small business owners report that their business is “very dependent” on automated processes. Another 27 percent say they are “somewhat dependent" on them. Many of these processes require timing/dating devices or computers. Automated processes are now spread throughout the economy and their malfunctioning would have wide repercussions. These processes are commonly associated with the manufacturing industry. The survey sample included too few manufacturers to report separately. However, the production industry of which manufacturing is an important component was the industry least likely to be dependent on automated processes. Both the distribution and service industries appear more dependent on them.

Malfunctioning computers also could severely impact small businesses. Exhibit 3 presents the frequency with which small business owners use computers for selected functions. The striking point of Exhibit 3 is the dependence on computers to perform multiple functions within the firm. In fact, small businesses with computers use them to perform an average of 5½ functions. Administration, record-keeping, and word processing is the most common application; operating machinery or equipment is the least.

EXHIBIT 3.—USE OF COMPUTERS FOR SELECTED BUSINESS FUNCTIONS AS A PERCENT OF SMALL EMPLOYERS WHO OWN COMPUTERS AND ALL SMALL EMPLOYERS

Function	Computer Owners (percent)	All small employers (percent)
Billing/Accounts Receivable	74	57
Inventory Control	41	32
Accounting/Gen. Ledger	76	59
Payroll	45	35
Admin/Record-Keeping/Word Processing	84	65
E-Mail/Internet Access	61	47
Customer—Prospect Lists/Sales Tracking	70	54
Design/Product Development	28	22
Operating Machinery/Equip.	20	15
Check Reconciliation	51	40

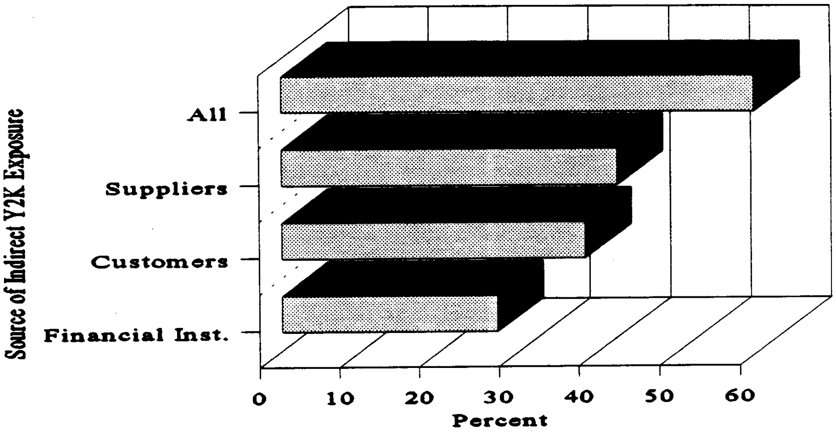
Software makes a computer run. It is generally believed that standard, off-the-shelf software packages are more likely to be free of Y2K problems than is custom software. A potentially important consideration and area for small employers to investigate then, is the kind of software they are using. Almost two of five owners who employ computers (39 percent) claim that at least half of their software is custom; 55 percent say that they use at least some custom products. Just 38 percent report that they use off-the-shelf software exclusively. The significant use of custom software in the mix magnifies small business exposure.

It is highly likely that more problems are buried in older software. In this sense, small business owners are in good position. Eighty-one (81) percent have updated their most critical software in the last two years. Only a handful have not updated in more than five. Owners of larger, small firms are more likely to have modernized than are the others.

2.2 Indirect Impacts

It takes two separate entities to make a business deal. Even if a small business does not have a Y2K problem, the other partner in the transaction may. The partner's problem may, therefore, force interruption or cancellation of a deal. Exhibit 4 examines some of these linkages and their subsequent problems. It shows that 75 percent of those with a computer (59 percent of small business owners) deal electronically with important business partners. Fifty-four (54) percent of small business owners with a computer (42 percent of the small business population) interact electronically with their suppliers. Eighteen (18) percent interact with them a lot. Thirty-five (35) percent of those using a computer electronically interact with their primary financial institution. Fourteen (14) percent interact a lot. Finally, 49 percent of small business owners with a computer interact electronically with their customers. Seventeen (17) percent do so frequently. Each of these are points of exposure to the Y2K problem could doom a potential transaction.

EXHIBIT 4.—PERCENT OF SMALL BUSINESSES WITH INDIRECT Y2K EXPOSURE BY SOURCE OF INDIRECT EXPOSURE



The indirect exposure to Y2K problems is broader than the numbers presented here. Survey figures only include fully electronic transactions. A number of business transactions occur which are electronic on one end but not on the other. An example might involve a small business owner placing a telephone order and the distributor processing it electronically. The primary implication is that the 75 percent noted earlier does not represent the full scope of indirect exposure of small business owners to Y2K. It must be amplified by partially electronic transactions which affect small business owners beyond those directly exposed and include practically everyone.

3. AWARENESS OF THE Y2K PROBLEM

Most small business owners claim to be aware of the Y2K problem. Fifty-three (53) percent say that they are "very aware" of it and another 28 percent say they are "somewhat aware." Just 8 percent are "not very aware" and 10 percent are "not at all aware." That means more than one million employers have limited or no awareness of Y2K.

One hopes that those most at risk (and with the capacity to take corrective action) are the same people who are most aware of the problem. The correlation between the two proves high, but not perfect. Eighty-six (86) percent of small business owners exposed directly are aware of Y2K, 59 percent are "very aware." Just 56 percent of those not exposed to direct risk are equally well aware. Thus, even if everyone is not aware, at least the overwhelming majority of the most vulnerable appear to be.

Though considerable awareness of the Y2K problem exists among small business owners, comparatively few of those aware believe the problem is serious for their business. Just six percent of those aware term Y2K a "very serious" problem and 23 percent of those aware call it "somewhat serious." Most see Y2K as a rather minor affair with modest or non-existent consequences. One respondent used the phrase, "blown out of proportion." In fact, 70 percent of aware small business owners term Y2K either "not very serious" or "not at all serious." Incorporating those not aware of Y2K, the number of small employers who believe the looming problem is negligible or non-existent approximates 77 percent of the small employer population or about 4½ million business.

Awareness of the Y2K problem does not necessarily translate into alarm or even concern. Those who claim to be "very aware" are no more or less likely than are others to believe Y2K is a serious problem. Efforts to increase general awareness of Y2K, therefore, will probably have little impact on a small business owner's level of concern over its impact. Instead, those wishing to stimulate action should shift the focus to the consequences for unprepared firms.

4. ADDRESSING THE Y2K PROBLEM

The number of owners who are taking action to address Y2K approximates the number who believe the problem is "very serious" or "somewhat serious." Twentythree (23) percent of those who are aware of the problem report action taken or in progress. Another 27 percent say that they plan to take action before 2000, though they have yet to initiate any. If this latter group follows through on its plans, one-half of small business owners who are aware of the problem will have taken steps to address Y2K in advance. That figure represents 41 percent of the entire small business population.

The relationship between the level of action and perceived severity of the problem suggests that perceptions change once action is taken. Exhibit 4 shows, as expected, that those who plan no action generally regard Y2K as "not at all serious" or "not very serious." Again, as expected, those who plan action, but have not yet taken, any consider the problem more serious than do those not planning any. The interesting group, however, is the one whose members either have taken action or are in the process of doing so. Owners taking action should be the group who consider the Y2K problem most severe, and indeed it produces the greatest percentage (15 percent) reporting the problem, "very serious." But, Exhibit 5 shows that the most frequent response (34 percent) from this action-oriented group is "not at all serious." One-third of those taking action think they have no Y2K problem to speak of. The remainder of responses among those taking action are distributed across the other possible answers. An explanation for this unexpected distribution is that action influenced their assessments. Once they acted, some owners learned the Y2K problem was very serious for their firms while other found it inconsequential. If that opinion occurs among those who acted, one could argue that a similar division of opinion will arise among those who have not yet moved but are exposed. A likely result is that some who take no action will not even notice 9/9/99 or 1/1/00 while others will be very unhappy.

EXHIBIT 5.—PERCEIVED SERIOUSNESS OF THE Y2K PROBLEM BY ACTION TO RESOLVE THE Y2K PROBLEM

	Problem seriousness				
Action level	Not at all serious (percent)	Not very serious (percent)	Somewhat serious (percent)	Very serious (percent)	Total
Not serious enough to worry about	70	25	3	2	100
No action taken/planned	46	34	18	2	100
Action planned	13	41	40	6	100
Action taken	34	24	27	15	100
Total	39	31	23	6	100

4.1 Expenditures on Y2K

The money spent by small employers taking action on the Y2K problem is comparatively modest. Twenty-nine (29) percent have made no outlays to date and another 27 percent have spent less than $1,000. ("No outlays" might consist of an inspection taken by in-house personnel.) Twelve (12) percent reported spending between $1,000 and $4,999. Thus, over ⅔'s of those taking action have expended less than $5,000. Another 13 percent don't know how much they have invested. These sums do not necessarily represent the entire cost, however. Thirty-nine (39) percent report plans for future outlays, though these investments will be generally small as well. Their expected median value is about $2,000.

The amounts spent on Y2K by owners taking action are notably less than their annual expenditures for computer equipment, software and maintenance. The annual median expenditure for these items is $7,500. Thus, much of their Y2K investment appears to have been made part of routine maintenance and upgrades.

Those planning action before the year 2000 intend to spend even less. Virtually none in this group (5 percent) have reported any expenditures to date. Their plans include 12 percent who anticipate spending nothing, 27 percent who plan to spend less than $1,000, and 20 percent who will spend between $1,000 and $4,999. One in three still doesn't know how much they will spend, leaving just eight percent of this group planning expenditures of more than $5,000. That is about the median annual expenditure among the group for computers, software and maintenance.

4.2 Plans to address Y2K

Plans to address Y2K often appear fragmented. The group taking action exhibits somewhat more structure in its approach to Y2K than those still planning it. The most notable differences between the two groups occurs in the areas of budgeting and verification of key vendor Y2K prevention steps. Small business owners taking action more frequently include a budget. Forty (40) percent of the action-oriented group have a budget for Y2K compared to 27 percent of the planning group. The planning group is more likely to check with key venders (49 percent compared to 32 percent). However, a majority do not have either element as part of their plans. Infrequent budgeting might be explained by the relatively small expenditures as well as the possible use of monies previously budgeted for computer maintenance and upgrades. The failure to check with key vendors can only be attributed to oversight or hesitancy to "interfere" in the internal affairs of another. Three of four from each group have designated a person to be in charge and somewhat fewer intend to test all changes made in response to Y2K.

Small business owners are about evenly split among those who will tackle the problem in-house and those who will contract it out. The ones who have taken action tilt toward keeping the task in-house. It is logical that those with expertise within their firms would be more likely to address the problem before others.

5. INFORMATION TO HELP SMALL BUSINESS OWNERS

Over half (58 percent) of the small employers who are aware of the Y2K problem believe that they have adequate information concerning the problem, its potential impact on their business, and how to protect themselves from any adverse consequences. At the same time, 47 percent indicate that additional information would be helpful.

Those most likely to feel that they have adequate information are found on both ends of the action continuum. Almost four of five (79 percent) owners who have taken action feel that additional information would not be helpful. Meanwhile, 62 percent of the small employers who aren't worried about Y2K feel the same. Those in the middle of the action continuum, particularly those planning action before 2000, are most likely to believe that they need more information.

Small employers say that the most helpful information would be a general description of the problem and the difficulties it may cause as well as information on specific remedies for the most common ailments. Previously, it was noted that there was a general feeling that the problem lacks importance. Therefore, information describing the problem needs to address consequences of inaction if it is to stimulate action. Few express interested in obtaining information containing the names and addresses of people or organizations that can help them resolve problems, or a detailed check-list of potential problem areas.

6. CONCLUSION

Virtually all save a healthy minority of the smallest, small businesses face direct exposure to a Y2K problem. Should their computer systems or other equipment/devices operated by a timing/dating mechanism malfunction, the consequences for about one in seven of those exposed are severe by the owners' own assessment. Though more than 80 percent are aware of the Y2K problem including most of those with the most serious exposure, just 23 percent of them have taken action to determine and correct the problem. Another 27 percent plan to do so prior to the year 2000. Thus, half of those aware of Y2K currently appear ready to leave their fate to the forethought (or lack thereof) of computer programmers.

The primary circumstance intervening between awareness of the Y2K problem and action appears to be the pervasive belief among small businessmen and women that Y2K is not a serious problem for their firms. Less than 30 percent believe the problem is "very" (6 percent) or "somewhat" (23 percent) serious. If the situation is not serious, the need to take action soon, if ever, is not a priority. Those attempting to help small business owners avoid Y2K problems, therefore, need to worry less about general awareness and focus on the likelihood and consequences of Y2K affecting their firms.

The survey data cannot yield an estimated Y2K impact for the small business population. Issues like the cost of substituting handwork for automation, average "downtime" during a malfunction, and the percent of firms exposed but not impacted are just three of the primary outstanding issues which are essential to the estimate and for which respondents could not provide reliable data. Still, the number of small businesses adversely impacted, if only modestly, will likely be very large. The survey shows that 4¾ million small employers are directly exposed with additional owners indirectly (and often unknowingly) exposed as well. It also shows that only half of the those aware of Y2K have taken or plan to take action in response. Thus even if all of those planning to take action follow-through and another million (about one in five of the exposed population) eventually make plans and carry-out preventive measures, over one million small, employing businesses will be directly exposed to the Y2K problem having taken no precautions.

7. SURVEY METHODOLOGY

The telephone survey on which this report is based was conducted during the latter part of April, 1998, by The Gallup Organization. The Dun & Bradstreet file constituted the survey's sampling frame. The sample itself was a stratified random design. Half was drawn randomly from owners of small businesses employing between one and 9 people (n=250); the other half was drawn randomly from those employing between 10 and 99 employees (n=250). Sampling error for the population is —4.4 percent. Unless otherwise noted, the data presented in the report are weighted to reflect the distribution of the entire small employer population.

YEAR 2000 (Y2K) PROBLEM

(Survey Results)

[Sponsored by Wells Fargo Bank, Conducted by The Gallup Organization in late April, 1998. Sample included small business owners employing from 1 to 99 people not including owners. n=500]

1. How dependent is the operation of your business on the use of computers? Would you say that your business is very dependent, somewhat dependent, not dependent, or you don't use computers in your business?

	Percent
Very dependent	44
Somewhat dependent	29
Not dependent	5
Don't use computers	22
Total	100

n=500

2. Do you have any equipment or devices in your business other than a computer that operate on an internal timing/dating mechanism or a micro-chip? Examples of such equipment might include automatic lighting and watering systems, elevators, scanning devices and card-readers. Do you have any?

	Percent
Yes	34
No	65
Dont know	1
Total	100

n=500

3. Do you sell, lease, or install as part of your business any devices that operate with an internal electronic timing/dating mechanism or a micro-chip?

	Percent
Yes	11
No	89
Total	100

n=500

3a. What portion of your sales involve those kinds of devices?

	Percent
All	10
More than half	29
About half	3
Less than half	38
Almost none	19
N/A	1
Total	100

n=53

4. How dependent is your business on automated processes? Would you say that your core business operation is very dependent, somewhat dependent, or not dependent?

	Percent
Very dependent	21
Somewhat dependent	27
Not dependent	49
Not applicable	1
Don't know	2
Total	100

n=500

5. If your computers, the devices operating on an internal timing/dating mechanism, automated processes, in your business were to malfunction, about what percent of your business sales or production would be lost for the period you were down?

Percent	*Percent* *Percent*
Less than 1	40
1–10	14
11–20	5
21–30	5
31–40	3
41–50	8
51–60	1
61–70	1
71–80	5
81–90	3
91–100	7
Don't know/refused	3
Not applicable	6
Total	100

n=408

6. Does your business use its computers for . . .?

	Percent
Billing and accounts receivable:	
Yes	74
No	26
Total	100
Inventory control:	
Yes	41
No	59
Total	100
Accounting and general ledger:	
Yes	76
No	24
Total	100
Payroll:	
Yes	45
No	55
Total	100
Administration, record-keeping, and word processing:	
Yes	84
No	16
Total	100
E-mail and/or Internet access:	
Yes	61

	Percent
No	39
Total	100

Maintaining customer and prospect lists and/or sales tracking:

Yes	70
No	30
Total	100

Design and product development:

Yes	28
No	72
Total	100

Operating machinery and/or equipment:

Yes	20
No	80
Total	100

Check reconciliation:

Yes	51
No	8
Don't Know	
Total	100

n=385

7. In a mix of custom and off-the-shelf software, would you say that your business uses all custom software, mainly custom software, 50/50 custom and off-the-shelf, mainly off-the-shelf, all off-the-shelf software?

	Percent
All custom	10
Mainly custom	7
50/50 custom and off-the-shelf	22
Mainly off-the-shelf	16
All off-the-shelf	38
Don't Know	7
Total	100

n=385

8. When was the last time your business updated its most critical software? Was it within the last 2 years, 2-5 years ago, 6-10 years ago, more than 10 years ago?

	Percent
Within the last 2 years	81
2–5 years ago	12
6–10 years ago	2
More than 10 years ago	1
Don't know	4
Total	100

n=385

9. What does your business spend annually for computer equipment, software and maintenance?

	Percent
Nothing	8
$1 to less than $1,000	26
$1,000 to $4,999	27
$5,000 to $9,999	14
$10,000 to $24,999	11
$25,000 to $99,999	4

	Percent
$100,000 or more	2
Don’t know	7
Total	100

n=408

10. How frequently do you interact electronically with your suppliers: a lot (frequently), a little (from time to time), not at all (never)?

	Percent
A lot (frequently)	18
A little (from time to time)	36
Not at all (never)	45
Don’t know	1
Total	100

n=408

10a. How critical is the use of computers to your SUPPLIERS’ operation? Is it critical, somewhat critical, not very critical, not at all critical?

	Percent
Critical	30
Somewhat critical	15
Not very critical	18
Not at all critical	28
Don’t know	10
Total	100

n=408

11. How frequently do you interact electronically with your primary financial institution: a lot (frequently), a little (from time to time), not at all (never)?

	Percent
A lot (frequently)	14
A little (from time to time)	21
Not at all (never)	64
Don’t know	1
Total	100

n=408

12. How frequently do you interact electronically with your customers: a lot (frequently), a little (from time to time), not at all (never)?

	Percent
A lot (frequently)	17
A little (from time to time)	32
Not at all (never)	51
Don’t know	1
Total	100

n=408

13. Are your sales PRIMARILY to private individuals or to other businesses and organizations?

	Percent
Private individuals	52
Businesses/organizations	40
Don’t know	8
Total	100

n=408

13a. How critical is the use of computers to your customers’ operations? Is it critical, somewhat critical, not very critical, not at all critical?

	Percent
Critical	40

	Percent
Somewhat critical	28
Not very critical	10
Not at all critical	11
Don't know	10
Total	100

n=164

14. Are you aware of something called the "Year 2000 Problem," often called the "Millennium Bug"? The problem involves a possible malfunction of some computer systems and similar devices on January 1, 2000. Would you say that you are very aware, somewhat aware, not very aware, or not at all aware with the year 2000 problem?

	Percent
Very aware	53
Somewhat aware	28
Not very aware	8
Not at all aware	10
Don't know	1
Total	100

n=500

15. How serious do you feel the Year 2000 Problem is for your business? Would you say that it is very serious, somewhat serious, not very serious, not at all serious?

	Percent
Very serious	6
Somewhat serious	23
Not very serious	31
Not at all serious	39
Don't know	1
Total	100

n=405

16. How do you intend to address the problem? Would you say it's not serious enough to worry about, no action has been taken and none is now planned, you plan to take action before the year 2000 but haven't yet, you have taken or are now taking action to address the problem?

	Percent
Not serious enough to worry about	22
No action taken and none is planned	24
Plan to take action, but haven't yet	27
Taken or are now taking action	23
Don't know	4
Total	100

n=405

16a. (Are you/will you) initially (addressing/address) the problem on your own or (are you/will you) (bringing/bring) in someone from the outside to help?

	Percent
In-house	47
Contract out	42
Don't know	11
Total	100

n=202

16b. Does your plan include . . . ?

	Percent
A budget:	
Yes	33
No	64

	Percent
Don't know	3
Total	100

A designated person in charge:

Yes	73
No	26
Don't know	1
Total	100

Testing any changes you make:

Yes	70
No	24
Don't know	6
Total	100

Checking on your key vendors to be certain they don't have a problem that affects you:

Yes	41
No	56
Don't know	3
Total	100

n=202

17. How much money has your business already spent addressing the Year 2000 problem?

	Percent
Nothing	64
$1 to less than $1,000	13
$1,000 to $4,999	7
$5,000 to $9,999	4
$10,000 to $24,999	3
$25,000 to $99,999	1
$100,000 or more	0
Don't know	8
Total	100

n=202

18. How much money does your business plan to spend, beyond what you have already spent, addressing the year 2000 Problem?

	Percent
Nothing	25
$1 to less than $1,000	21
$1,000 to $4,999	17
$5,000 to $9,999	5
$10,000 to $24,999	2
$25,000 to $99,999	2
$100,000 or more	1
Don't know	29
Total	100

n=202

19. How will your Year 2000 plans impact your sales? Do you think it will increase, decrease, or have no impact on them?

	Percent
Increase	10
Decrease	3
No impact	84
Don't know	3
Total	100

n=202

20. How will your Year 2000 plans impact your employment level? Do you think it will increase the number of people working for you, decrease the number, or have no impact?

	Percent
Increase	7
Decrease	1
No impact	90
Don't know	1
Total	100

n=202

21. Have you verified that your suppliers and financial institutions are taking steps to prepare for the Year 2000?

	Percent
Yes	32
No	65
Don't Know	3
Total	100

n=405

22. Have you verified that your customers are taking steps to prepare for the Year 2000?

	Percent
Yes	13
No	83
Don't know	3
Total	100

n=405

23. Do you believe that you have adequate information about the Year 2000 Problem, its impact on your business, and how to protect yourself from any adverse impact?

	Percent
Yes	58
No	39
Don't know	4
Total	100

n=405

24. Would you be very interested, somewhat interested, not very interested, not at all interested in learning more about the Year 2000 Problem and how it might affect your business?

	Percent
Very interested	12
Somewhat interested	35
Not very interested	14
Not at all interested	39
Total	100

n=405

25. What type of information about the Year 2000 Problem would you find most helpful?

	Percent
A general description of the problem and the difficulties it may cause	31
Specific remedies for the most common possible problems	22
How it would affect financial institutions (volunteered)	5
Names and addresses of people or organizations that can locate or help resolve possible problems in your business	4
How it would affect my business (volunteered)	4

	Percent
A detailed check list of possible problem areas	3
Other	6
Don't know	20
Nothing	5
Total	100

n=247

DEMOGRAPHIC PROFILE OF RESPONDENTS

D1. Which best describes the majority of your business activity? Do you make, construct, extract or grow something to sell; sell goods or products; sell services?

	Percent
Make, construct, extract or grow something to sell	12
Sell goods or products	29
Sell services	56
Don't know	3
Total	100

n=500

D2. Which BEST describes the area in which your business is located (main headquarters)? Is it located in a city and surrounding suburbs with more than 500,000 people, city and surrounding suburbs with 50,000 to 500,000 people, city of less than 50,000 but more than 5,000, community of less than 5,000 or a rural area?

	Percent
City and surrounding suburbs with more than 500,000 people	29
City and surrounding suburbs with 50,000 to 500,000 people	28
City of less than 50,000 but more than 5,000	20
Community of less than 5,000 or a rural area	20
Don't know	1
Total	100

n=500

D3. How many people do you employ?

	Weighted (percent)	Unweighted (percent)
1–4	57	35
5–9	20	12
10–24	14	28
5–99	8	23
Don't know	2	2
Total	100	100

n=500

D4. During your last fiscal year, were your sales less than $250,000; $250,000 to less than $500,000; $500,000 to less than $1 million; $1 million to less than $2 million; $2 million to less than $5 million; $5 million to less than $10 million; $10 million or more?

	Percent
Less than $250,000	42
$250,000 to $499,999	18
$500,000 to $999,999	10
$1 million to $1,999,999	12
1$2 million to $4,999,999	4
$5 million to $9,999,999	3
$10 million or more	2
Don't know	9
Total	100

n=500

D5. How long have you owned or operated this business?

	Percent
Less than 6 years	27
6–10 years	23
11–20 years	28
21+ years	20
Don't know	1
Total	100

n=500

D6. Please tell me your age?

	Percent
Under 30	4
30–39	18
40–49	31
50+	45
Don't know	2
Total	100

n=500

D7. Gender?

	Percent
Male	74
Female	26
Total	100

n=500

Responses of William J. Dennis to Questions Submitted by Chairman Bennett

Question. Mr. Dennis, I find your testimony is unnecessarily leaning to the optimistic side. The Wells-Fargo sponsored survey, which samples approximately 4.8 million small employers, brings out these facts, and correct me if I'm wrong:

—almost ⅓ of small employers reported that they would lose over 30 percent of their sales or production for the period their computers and automated processes were down. That translates to well over 1 million small employers who are doing at best 70 percent of the business they were doing before Y2K problems hit.

Do you think it is appropriate to focus only on the extreme cases which is the 330,000 or so businesses you refer to in your testimony? Wouldn't most small employers consider losing over 30 percent of sales or production significant? For instance, in this city, a large number of small vendors and eateries folded just due to the three week Government furlough in 1995.

Answer. Your point is well-taken. Small businesses do not have to be completely shut-down in order to experience significant adverse impacts. This is particularly true if the loss of sales/production occurs over an extended period. In fact, the length of the loss may be more critical than the daily percentage of loss. For example, if a small business owner lost 100 percent of sales or production for a day, he would be unhappy. If he lost 30 percent for a month, he could be in serious trouble. Unfortunately, we could not ask a question on the survey about duration of downtime and expect an informed response.

The report specifically notes that the difficulty with waiting until January 1, 2000, to resolve a Y2K incident is that a small business owner probably will not be able to get anyone to fix the problem right away. Other customers, probably large businesses and governments, will have all the qualified locked-in. The small business will have to hobble along. When it finally does get someone in, the cost will be significantly higher than it would have been. The unknown length of downtime is, I believe, one of the strongest arguments for action.

Your one-third calculation is not quite correct. That figure covers the population with direct exposure including those who have and have not taken action. Including only those who have taken no action and who do not plan any, the number directly impacted is under one million. Still, that is a very large number, large enough to create considerable concern.

Question. You state that over 80 percent of small employers are exposed to Y2K problems though their computers, but a majority of them plan no action as of the survey done in April of this year. You also say that ″government isn't particularly credible with small business owners nor are its communications.″ You do suggest working with trade associations to spread the Y2K message, but I'm wondering if this alone is sufficient. Can you provide the Senate with any suggestions that the Congress can take action on?

Your written statement astutely points out that small employers have indirect exposure to Y2K problems as well as direct exposures, for instance with a customer or supplier whose computers the small employer must access. You estimate that this may extend to practically all small employers. Yet we learn from other parts of your statement that this group is particularly in the dark on the Y2K issue and is likely to remain so. This is very troubling. What can be done to get this very important part of our economy to pay more attention to this issue that may cripple them in just 450 days from now?

Answer. The two most influential groups for small business owners are industry-specific trade associations and peers. Small businessmen and women are most likely to listen to and respond to these two groups.

I have no doubt that the Committee could exert considerable influence on industry-specific associations through direct communication. The same would be true for local organizations whether as large as the Washington Board of Trade or neighborhood business organizations. This is no mean task. The Encyclopedia of Associations lists thousands of them. But I think it would be a useful endeavor. Further, small business owners will probably be more receptive to the message as January 1, 2000 approaches. They usually face a myriad of business problems. Y2K is just one of them. So as the deadline nears, owners will be paying more attention.

The second thing that you can do is to encourage larger firms and state and local governments to use their pulpits. They do business with millions of small firms. They could certainly provide a public service by doing as little as enclosing a letter about Y2K to their customers and suppliers.

I would not expend my resources on media events or national campaigns in the traditional sense. Who has enough credibility and visibility to be taken seriously? Y2K is a business problem and political leaders lack credibility with Main Street on such matters.

It is also important that the Committee or any other group make a credible case. As the survey shows, a large number of owners simply do not believe either that a problem exists or that the Y2K problem is serious enough to warrant attention. That means they need information clearly outlining the costs and consequences of not taking preventive action. For example, if I believe that I can replace an infected computer and software for $2,000 and that a consultant will cost $1,000 to tell me I have a problem, then why shouldn't I adopt a wait and see attitude? That is a reasonable risk. But if you tell me, the problem will screw-up my records, perhaps irretrievably, and that I probably won't be able to get anyone to come in and fix what I have left for a month, you have my attention.

Though the data do not show it, I personally believe that a substantial number also simply don't know where to begin. Many owners are not comfortable with the technology. To draw an analogy, they can drive it productively but don't ask them what's under the hood or how it can be fixed.

PREPARED STATEMENT OF SENATOR CHRISTOPHER J. DODD

Thank you, Mr. Chairman, for holding this hearing. As you mentioned, this is the ninth hearing that this Committee has held. You have frequently compared your role in the Y2K issue to that of Paul Revere, but you, Senator Bennet, have logged far more hours than that legendary patriot. We know that the Y2K threat is coming. We know the time remaining between now and the turning of the millennium to the second. We know we must alert our citizenry. If the polls are correct, and if only a small percentage of Americans have heard of the year 2000 computer problem, then we have an extraordinary task at hand.

This Committee has held eight hearings, covering such wide ranging subjects as electricity grids, health care, financial markets, telecommunications, emergency services, pensions and mutual funds, and now we come together to examine small and large businesses.

Perhaps the single most important message coming out of these hearings is that the hour is late and the vast majority of the planet is not prepared. That the United

States leads the world in Y2K remediation is a thin silver lining when our hearings indicate that many sectors within the United States are not prepared, or just starting their Y2K planning. Just one of many areas that deeply concerns me is the small business sector. Many small businesses are either unaware or unconcerned about the Y2K problem. Yet they are crucial to the welfare of the American economy. They employ nearly 18 million American workers. They provide 51 percent of the private sector output. Despite the label "small business," they are by no means small in their importance. Whether they realize their role in our Y2K challenge is, unfortunately, another matter. Small businesses seem to think that they can hide from the Y2K problem. In a recent Wells Fargo Bank survey of small business Y2K preparedness, 81 percent of small businesses surveyed knew of the problem, but no more than 25 percent had acted on that information. This is unacceptable.

I would like to borrow one of Senator Bennett's metaphors which compares this committee to the National Weather Service. We have a worldwide Y2K storm brewing which, unlike the tropical storms and other disasters that the National Weather Service tracks, is at least partially controllable. We still have more than a year to identify the most critical systems and fix them. Unfortunately, we still lack the kind of international storm warning and response system that this issue requires. We need an international focus that can identify the global risk and take appropriate action to protect our interests in energy, food supplies, critical commodities and manufactured products. Until we see this kind of joint domestic and international participation, the Year 2000 technology problem will continue to pose a significant physical and financial risk to American and international citizens alike.

Interconnectivity is another appropriate theme for this hearings. Almost all business sectors have some common Y2K factors such as computers, software and microprocessors. As we examine each industry in detail we are discovering that interconnectivity between businesses is one of the greatest issues we face. Most businesses are dependent on their suppliers, distributors, and customers through some means of electronic data interchange. The digital device that sends and receives these messages is connected to some kind of computer or microprocessor that is run by software, any part of which may not be Y2K compliant. It only takes one part of the link to break for the exchange of data to come to an abrupt halt. Thus the hard work of many internally Y2K compliant companies could be for naught if their suppliers and distributors are not in synch with their respective Y2K remediation efforts. We look forward to today's witnesses discussing this issue with the committee.

The Senate as well as the American public have a keen interest in monitoring the response levels that public and private organizations have displayed with respect to the Y2K problem. Most are aware of their civic duties, and have volunteered to tell the Y2K story, recognizing that their experiences will be useful to others. But there are other companies and industries that willfully and knowingly chose not to cooperate with our efforts. In many cases, these are companies whose products are essential for the day-to-day existence of the average American. For example, many major representatives of the food industry have decided that it is not in their best interest to tell the public the Y2K status of their industry. Their industry associations were equally unsupportive.

Based on the eight hearings that preceded this one, we have arrived at a fairly clear picture of our Y2K strengths and weaknesses. In general, all those affected with the Y2K bug have arrived at the party well beyond "fashionably late." However, today's hearing provides us with one more opportunity to improve our response time for the ultimate deadline, the one just 450 days away. The pharmaceutical industry will give us a complete picture of what it means when we talk about Y2K readiness. Their testimony highlights the extremely complicated and interconnected supply lines that provide millions of Americans with essential prescription drugs.

The pharmaceutical industry includes a large international component. For example, diabetics can live long and healthy lives with the help of regular doses of insulin, a substance that is mainly produced in Denmark. If Denmark's insulin production is affected by the Y2K bug or any other disaster, the thousands of Americans that depend on this drug to control their diabetes will find themselves in grave danger. Insulin is just one product that embodies the interdependent nature of the world in terms of business and economics, as well as health and social welfare. We hope the Danes, and the rest of the international community are as concerned about Y2K as we are. Steps must be taken to insure that the factories that produce insulin, and other such life-saving drugs can function properly after January 1, 2000.

The spectrum of American business centers around major producers, much as it has since the invention of commerce. If business history teaches us anything, its is the symbiotic relationship between large and small businesses. Large corporations need small companies to tailor the delivery of goods and services to meet consumer needs. This morning we will see Y2K issues from both ends of the business spectrum. Representatives of the 5 million small businesses, most with less than 500 employees, have the unique challenge of meeting Y2K obligations which, in some cases, may be just as large as the ones facing companies with tens of thousands of employees.

Again, thank you Mr. Chairman for your leadership, and thank you to our witnesses for their cooperation.

PREPARED STATEMENT OF HON. FRED P. HOCHBERG

Thank you, Mr. Chairman, for inviting the U. S. Small Business Administration (SBA) to testify before the Senate Special Committee on the Year 2000 Technology Problem. My name is Fred P. Hochberg, Deputy Administrator of the SBA, and I am here today on behalf of Administrator Alvarez, who joins me in welcoming the opportunity to discuss the so-called "Year 2000" or "Y2K" problem facing the nation's 23.6 million small businesses and their customers. We also look forward to providing information to the Committee on SBA's efforts to improve awareness of this problem and to minimize its impact on small businesses.

We at the SBA take the Year 2000 issue very seriously and the President has directed SBA to take a lead role in addressing this concern as it affects small business. The full extent to which the Year 2000 bug may affect businesses is unknown. However, it is clear that the damage can be minimized with foresight and preparation. My testimony consists of two parts—what SBA is doing to insure that our own computer systems are Y2K compliant and what SBA is doing to help our customers understand the problem and have some information on how to address it in their own businesses.

SBA'S COMPUTER SYSTEMS

The SBA's Year 2000 awareness efforts actually began in 1996 when we realized that, in order to better serve small businesses, we should improve our own internal computer protections. I am pleased to inform you that as of September 1998, we have completed the renovation of the computer programs in all of SBA's mission critical systems. By the end of October we will have completed the validation and implementation of these programs—well ahead of targeted goals for the federal government. Our non-mission critical systems also have been identified and, currently, we are working with our field offices to continue corrections of local systems in these offices.

We are quite proud of the fact that the SBA was one of only three agencies to earn an "A" for our Y2K work when the House Committee on Government Reform and Oversight's Subcommittee on Government Management, Information and Technology issued its report card last month on the Federal Government's progress in addressing the Y2K issue.

Because we are ahead of schedule, we plan to conduct additional systems integration and data exchange testing during the first quarter of fiscal year 1999. We will correct any identified problems by the end of the second quarter.

To avoid taking anything for granted, we have established a Business Continuity and Contingency Planning Committee. I chair this committee and it is composed of the SBA's top managers. Our goal is to ensure that SBA is prepared to deliver its services regardless of whatever problems we may encounter as a result of the Y2K issue.

SBA IS SEEKING WAYS TO HELP OUR CUSTOMERS

Once our internal improvement efforts were underway, we turned our efforts towards the private sector. We wanted to bring the seriousness of this problem to the attention of small business owners without creating undue panic. In addition, by educating small businesses that they could have a problem, we sought to prevent them from making any unnecessary expenditures toward fixing this problem.

Initially, many people—including the SBA—believed users of new desktop hardware with off-the-shelf or "shrink-wrapped" software would be protected from the Year 2000 problem. SBA convened two separate industry review groups. The first consisted of the mainframe computer and independent software industries and the second represented desktop computer manufacturers and "shrink-wrapped" software producers. They helped correct our perceptions of the Y2K problem and gave us suggestions on how to present the problem to the small business community (Participants listed in Attachment 1). These review groups were instrumental in helping the SBA develop steps businesses can take to better prepare themselves to address the Y2K problem.

The experts told us that even recently purchased equipment could be threatened by the Y2K problem. Validated systems may not actually be Year 2000-compliant if users have modified them by entering non-compliant data.

In addition, there may be telecommunications problems associated with the failure of microprocessors or "embedded chips" that are date-sensitive. This could affect credit card readers, automatic teller machines, fax machines, pager and e-mail service. Other items of concern to small businesses could be the possible chip-related failures of heating and ventilation systems, security alarms, and even elevators.

YEAR 2000 AWARENESS PROGRAM MESSAGE

As a result of our work with the industry experts, we developed the following advice that anchors our Y2K outreach efforts.

First, businesses are encouraged to conduct a self-assessment to see if they may have affected computer hardware and software, as well as any electronic equipment using date-sensitive embedded computer chips. Operating systems, like DOS or Windows, should be evaluated for their vulnerability to the Year 2000 bug. Products like Lotus 1–2–3, Oracle, or Excel, which may contain date-reliant data, should also be reviewed.

We are aware that it is not enough for small businesses just to take care of their own Y2K problems. They need to assure themselves that the companies in their supply and distribution network are also Y2K compliant. As we continue to revise and enhance our message to the small business community, we will encourage them to develop contingency plans for keeping their businesses operating. We believe this a very prudent action to take for ensuring business continuity in the event their normal suppliers or other supporting vendors are unable to provide the products and services they need.

This is not just a computer problem, however, as other equipment with embedded computer chips could also be at risk. Anything that uses a calendar or date record should be assessed. Thorough assessment of elevators, machinery and other mechanized systems is key. The theme of this message is that it is not too soon to begin evaluating one'*s vulnerability to the Year 2000 threat.

Second, businesses are encouraged to take action immediately. Corrective actions could range from a change in software to hiring a consultant to repair any problems. Repairs may not necessarily be expensive and we are encouraging businesses to contact their computer hardware and software vendors first. Fixing any Y2K problems discovered in the self-assessment is a must, and testing the repairs is vital. Upon completion of repairs, businesses must test and re-test to assure they won't have any problems. Having a contingency plan is also necessary because businesses can never be sure if their vendors and other contacts are themselves compliant.

Third, businesses are encouraged to stay informed about this issue. Accurate Y2K compliance information could change and business owners should keep abreast of any modifications they may need to make in their equipment or operations. A change in Year 2000 compliance by one business, regardless of size, could have a ripple effect for smaller businesses that rely upon its services or supply inventory. Visiting various Internet Y2K websites is a great way to stay current.

These steps form the basic context of our public awareness program. We have prepared materials and media to notify small businesses about the Y2K issue. They include posters, flyers, a fact sheet, a public service announcement (PSA) and phone hotline. Each of these provides basic information and refers people to the SBA website (www.sba.gov). The website features information on how businesses can protect themselves from the Year 2000 problem (Attachment 2). The website also provides "hyperlinks" to major computer hardware and software manufacturers and distributors to aid individuals in safeguarding their equipment and software from the Y2K Problem. Since its inception in February 1998, the site has been "hit," or visited, over 840,000 times.

Additionally, the SBA is making information available through a new toll-free phone number, 1–877–RUY2KOK. Started on June 23, 1998, the phone line is an automated "fax-back" system which allows callers to have Year 2000 information faxed back to them at the conclusion of the call.

YEAR 2000 AWARENESS PROGRAM OUTREACH

Our coordinated national awareness program asks small businesses "Are You Y2K OK?" Our traditional resource partners, such as our lending partners, Small Business Development Centers, SCORE volunteers and small business trade associations, in addition to our private sector supporters, have agreed to help spread our message. For example the American Bankers Association included all of our materials in their Year 2000 member resource guide. We look forward to working with the private sector to leverage our resources, experience and knowledge with the Y2K issue to help small businesses become compliant. Since our Year 2000 kick-off in early June, SBA's efforts have resulted in numerous public forums with SBA representatives reaching a broad radio and TV audience.

In addition, the SBA has conducted Y2K training events across the country. Together with IBM and the U.S. Chamber of Commerce, the SBA has developed a full-page advertisement on Y2K preparedness, to be published in Nation's Business Magazine this month. As a result of the emphasis we have placed on this issue with our district offices, the SBA's Y2K awareness campaign has been featured in more than 200 metropolitan and local newspapers since June. Administrator Alvarez was recently featured in a Y2K piece by Fortune magazine.

Since June, we have distributed more than 2 million Y2K flyers through our private sector partners, such as financial institutions, power companies and newspapers. We are also very excited that we recently reached an agreement with the Internal Revenue Service to distribute nationwide, through their next mailing to small business owners, 6.5 million copies of our "Are You Y2K OK?" flyers. Requests for our "Are You Y2K OK?" materials, as well as for public service announcements and general Year 2000 information, continue to pour in. We are committed to meeting these requests and have plans to update our material later this year.

The SBA continues to work hard to build alliances with trade and industry associations. We believe it is important to have as much help as possible in carrying our Year 2000 message.

Y2K ACTION WEEK

Before I conclude my testimony, let me tell you about an exciting activity we have planned for later this month. We will sponsor a nationwide initiative during the week of October 19th to focus government, business and media attention on the Y2K problem. During that week, we are asking all of SBA's district offices and resource partners to sponsor at least one major Y2K awareness event. It is our hope that we can reach literally tens of thousands of small businesses during this week and motivate them to take action now on this serious management issue.

We have received strong support from John Koskinen and his staff at the White House Y2K Office and will be joined in this effort by the Departments of Commerce, Agriculture, Interior, Transportation, the Social Security Administration, Internal Revenue Service and the U.S. Postal Service. Attendees at these events will then take the message back into their local communities. We hope that this issue will then be raised at local chambers of commerce and other business organization's meetings to assist us in getting the work out to the small business community.

CONCLUSION

As we update both our material and our messages, we plan to continue encouraging small businesses to stay informed on this issue. Business owners can get up-to-date information by reading the newspapers, watching the nightly news, visiting the SBA website (www.sba.gov) and other websites and contacting their vendors. The best defense is staying informed and taking action accordingly. And most important, everyone needs to take action now; it is too late to start early. We recognize that some businesses may be Year 2000 compliant already. However, the risks are too great not to check. Small business owners need to make informed decisions about this issue.

The reaction to our efforts has been overwhelmingly positive. We both need and appreciate the support we've enjoyed from Congress as well as the businesses and trade groups who have allied themselves with our effort. As you return to your respective states in the coming weeks for town hall meetings and other public gatherings, we urge you to carry forward the Year 2000 message. We are happy to provide materials or help you communicate with your small business constituents any way we can. The Year 2000 issue can be managed if businesses take responsible action now while there is still time.

Thank you, Mr. Chairman, for inviting the SBA to testify. I look forward to working with you. I will be happy to answer any questions.

[ATTACHMENT 1]

PARTICIPANTS IN SBA YEAR 2000 FOCUS GROUP I, MARCH 30, 1998

Mr. John Koskinen, Assistant to the President, Chair, President's Council on Y2K Conversion

Mr. Jim Morrison, Senior Analyst, National Association for the Self-Employed
Ms. Heidi Hooper, Y2K Program Manager, Information Technology Association of America
Mr. Anthony W. Powell, President, Anthony W. Powell, Inc.
Mr. Alton Turner, Next Millennium Consultant. Inc.
Mr. A. Nayab Siddiqui, President, Scientific Systems & Software International Corporation
Mr. Jim Berish, Government Affairs, Hewlett Packard
Dr. Kam F. Tse, Contemporary Technology, Inc.
Mr. Andrew Pegalis, Next Millennium Consultant
Mr. Scott Davies, Y2K Executive, Global Government Industry, IBM Corporation
Mr. Bob Cohen, Vice President of Communications, Information Technology Association of America
Mr. Bob Price, Corporate Y2K Manager, Digital Equipment Corporation
Mr. Robert Wagman, Executive Editor, Millennium Information Service
Mr. David Voight Director, Small Business Center, Chamber of Commerce
Mr. Mike Roush, Small Business Technology Coalition
Ms. Susan Tuttle, Program Manager, IBM
Mr. David Y. Peyton, Director, Technology Policy, National Association of Manufacturers

PARTICIPANTS IN SBA YEAR 2000 FOCUS GROUP II, APRIL 23, 1998

Ms. Moira Praxedes, Systems Analyst, Gateway 2000
Ms. Lynn Silver, Senior Education Policy Manager, Apple Computer, Inc.
Ms. Deborah Morse, Y2K Coordinator for Corel Products, Corel Corporation
Mr. Dave Cunningham, Program Manager for Y2K, Dell Computer Corporation
Ms. Beth Land, Corporate Strategist, Novell Corporation
Mr. Rolin Hua, Vice President, Corporate Development SMAC Data Systems
Mr. Ted Graig, Government Account Representative, Microsoft Corporation
Mr. Roger Geides, Business Development Manager, Microsoft Corporation
Mr. Scott Davies, Y2K Executive, Global Government Industry, IBM Corporation
Mr. Mike Roush, Small Business Technology Coalition
Ms. Heidi Hooper, Y2K Program Manager, Information Technology Association of America
Ms. Nancy Peters, Information Technology Association of America
Mr. David Voight, Director, Small Business Center, U. S. Chamber of Commerce
Ms. Deborah Spencer, Technical Account Manager, Lotus Development Corporation
Mr. Bernie McKay, Intuit Corporation

[ATTACHMENT 2]

THE YEAR 2000 PROBLEM

ARE YOU READY TO DO BUSINESS IN THE YEAR 2000?

If you think you are, have you completely tested all your systems to make sure you won't have problems? Have you talked to your business suppliers and other business partners to ensure that they are ready? Whether or not you are ready, we invite you to reviewthis document on year 2000 readiness.

WHAT IS THE YEAR 2000 PROBLEM * * *

The year 2000 problem started decades ago when earlycomputers had very limited memory and storage space. Programmers saved space where they could by storing the absolute minimum amount of data necessary for business functions. One place they saved space was the date, in which years were represented by their last two digits. So, 1946 was represented and stored as 46, 1967 was stored as 67, and so forth.

Reducing years to two digits works well as long as the century does not change. As the next century approaches, however, computers that still maintain years as two digits may not recognize that the year 2000 is greater than the previous year. Although a computer may recognize that 99 is greater than 98 (as in 1999 and 1998), it may not recognize that 00 is greater than 99 (as in 2000 and 1999) and may consider it 1900.

AND WHY IS IT SO IMPORTANT?

Data processing systems used in all types of businesses rely heavily on dates and date processing. If the computer code does not recognize that one date is greater than another, it may not be able toprocess properly and may produce erroneous results. For example, if a loan is entered into a program with a start date of 1998 and a payoff date of 2005 (98 and 05), the program may subtract 98 from 05 resulting in a term of −93 years, rather than 7 years. This problem may put a business at risk because it could effect its cash flow, inventory, taxes, interest calculations, financial forecasting,customer relations, and many other areas.

HOW BIG A PROBLEM?

This worldwide problem not only affects mainframe computers and their programs, but also personal computers and every piece of hardware that contains a microchip, including:

—manufacturing control systems
—telecommunications
—money transfer and other financial systems
—gas, water, and electrical utilities
—stock markets
—transportation
—national defense
—home computers, security systems, and appliances

Beyond your own business computer systems, there is also the "business supply chain." You buy goods and services from some businesses, and you sell goods and services to others. If your trading partners fail, your cash flow can suffer critically.

In 1996, the Gartner Group estimated that the year 2000 problem would cost $600 billion to fix. Later estimates by Lloyds of London have been as high as $1 trillion. Economist Ed Yardeni has estimated that there is a 35 percent chance of a global recession because some businesses will be unable to deal with their year 2000 problems. And, unlike most projects, the final due date can not be changed with the year 2000 problem—the year 2000 will arrive whether we areready or not.

NO "SILVER BULLET"

According to Peter de Jager, an internationally recognized expert in the year 2000 problem, there is no single solution, no so-called "silver bullet." Because each system processes dates in different ways, each system must be assessed and corrected.

YOU CAN'T DO NOTHING

If you do nothing to fix this problem, your business may fail. Worse, because the year 2000 problem is a foreseeable problem, the officers and directors of your organization could be held personally liable in shareholder suits.

The Federal Reserve recognizes that small businesses are the backbone of the economy and wants to ensure your business's continued good health. With estimates predicting that 1 percent to 7 percent of U.S. businesses will fail because of the year 2000 problem, the Federal Reserve is encouraging all businesses to address the problem as early as possible.

YOUR BUSINESS IS AT STAKE

Imagine if you were unable to retrieve your accounts receivable records, or if one of your customers placed an order with you in late 1999 for delivery in early 2000, and that order was lost. Imagine if you could not correctly calculate the taxes or insurance premiums to be withheld for your employees, or if your inventory records were lost.

The year 2000 problem may affect your business in countless ways. Your personal computers may reset themselves to the year 1980 or 1900 because the microchip that maintains the clock/calendar does notrecognize 2000 as a valid year. A photocopier that records the count of the number of copies made in a day may stop working in the year 2000 because the microchip may fail to recognize that "00" is a valid year. A security system may fail to operate properly and might allow unauthorized access to your buildings. A preprogrammed fax machine used to send announcements to your customers may stop working after 12/31/1999. A voice mail phone system may fail to record messages from customers or suppliers. A preprogrammed money transfer from a savings into a checking account to cover checks to your creditors may not take place.

Reports of year 2000 problems are already surfacing in the media. In early August 1997, the owners of a grocery store chain in Michigan sued the manufacturer of their cash registers because the terminals would not recognize credit or debit cards with an expiration date of 00. The owners claimed they had lost thousands of dollars worth of business because the terminals rejected customers with valid debit/credit cards.

IT'S NOT JUST A DATA PROCESSING PROBLEM

The year 2000 problem is a business problem. The decisions to spend the money, time, and resources are business decisions. The costs of making your organization compliant may be substantial, so the decisions on what to fix and what to risk not fixing need to be made at the highest levels.

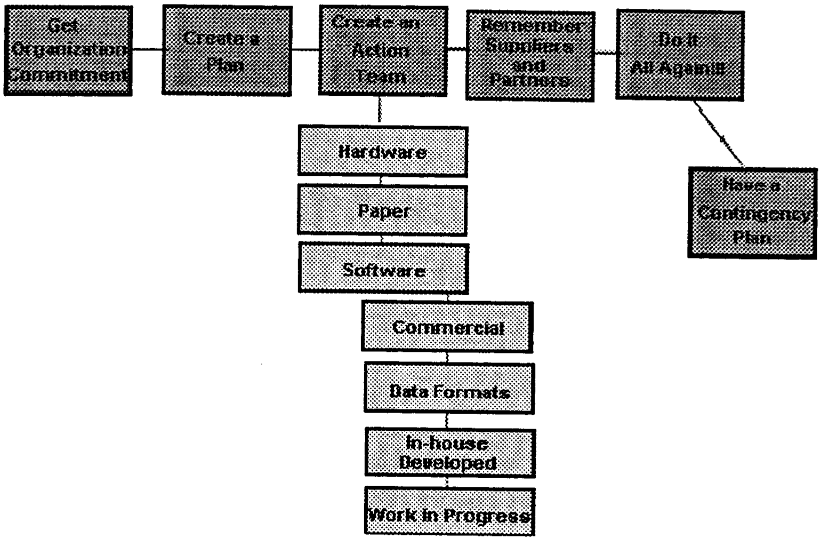
MANAGING TO YEAR 2000 READINESS

Correcting the year 2000 problem in your organization will require senior management involvement. The Board of Directors should be involved. You may want to form a year 2000 team, and include legal and audit representatives. If appropriate to your business, you may want to designate one person as your year 2000 project manager with responsibility for making your entire business ready for the century date change. You may also want to designate one person in eachfunctional area as a year 2000 coordinator or representative with responsibility for tracking that area's readiness activities. Year 2000 readiness must be made a priority from the top down.

An overall project plan with milestones and deadlines will be critical to your efforts. Each functional area should be encouraged to develop its own plans.

Hint—A project planning and tracking tool, such as Timeline® or Microsoft® Project, will help you track tasks that are due to start, past due, or are on the critical path.

Y2K STEPS TO TAKE



Y2K Checklists for Small Business

No single Y2K checklist fits everyone's needs since businesses have a wide variety of services and technologies. We are offering several that focus on small business needs, starting with the one below from the Federal Reserve Board. Links to additional checklists, definitions, and resources are provided as well. This page is a "work in progress" and will grow as we come across more information. Keep in mind, there are many excellent checklists on the Internet. Browse the internet and if you find one you like, let us know!

SUGGESTED STEPS TO READINESS

The most important first step is to develop a strategy to make your business ready for the year 2000. Many consulting firms have developed different strategies with 3 to 15 steps to take to help companies deal with the year 2000 problem. Information about these different plans can be found on the Internet or in trade journals.

Here is a simple five-step plan to achieve year 2000 readiness.

(1) Awareness—educating and involving all levels of your organization in solving the problem

A crucial step in awareness is creating a communication strategy to make certain that everyone is informed and that management has the information it needs to make decisions. Holding seminars or meetings to educate people and bringing in outside speakers are two ways to increase awareness.

A critical aspect of awareness is to develop an internal standard for year 2000 readiness. The Federal Reserve uses the following definition: "Systems (e.g., software, hardware, firmware) are defined as ready if they can demonstrate correct management and manipulation of data involving dates, including single-century and multi-century formulas, without causing an abnormally ended scenario within the system or generating incorrect values involving such dates."

The awareness phase never ends. As people move to other jobs, and new people are hired, they must be educated. There is also an ongoing need to keep your staff and business partners informed.

(2) Inventory—creating your checklist toward year 2000 readiness

In this phase, you should identify and list all of the different computer-based systems, components (such as in-house developed systems, purchased software, computers and associated hardware), service providers, and hardware that contain microchips that support your business. Each entry on your list should be ranked by how critical it is to your business.

Indicate on your inventory whether the component is hardware, software, or a service. It may be useful to note which components support your telephone or data communications networks. If a computer-based system uses a vendor-supplied package, record the name of the vendor and the release number, if known.

Hints—Keeping your inventory on a spreadsheet or database makes it easier to sort and report on items that are not ready. It is also helpful to develop an identification system to help track components. For each item on the inventory, assign a person who will be responsible for assessing that item and preparing for the year 2000.

Reminder—Some systems will begin failing before the century date changes because they perform forecasting or future processing. This is called "time horizon to failure" and should be considered during inventory and assessment. The "time horizon to failure" should be listed on your inventory if it is known.

(3) Assessment—examining how severe and widespread the problem is in your business and what needs to be fixed

Starting with the most critical items on the inventory, determine which systems are date-sensitive and if they will fail when the century changes. Systems with an imminent "time horizon to failure" should also be assessed first. A date-sensitive system is one that manipulates or works with dates in some way, or a system that operates differently based upon the date. Please refer to the questions later in this brochure to keep in mind when assessing your systems.

Examples of date-sensitive systems include ones that perform any kind of forecasting or projections through time, such as calculating interest on a loan or projecting inventory levels. Other examples of date-sensitive systems are those which retrieve records based on a date (such as invoices), or systems that sort items by date (such as accounting or inventory systems). Examples of date-sensitive hardware include lighting systems that switch on automatically on weekdays, manufacturing control systems, and scanners or card readers that read ID badges or credit/debit cards.

One way to assess a system is to look at the computer code and follow the logic. If this is not possible because the system is based on a purchased package, you should contact the vendor.

Another way to assess a system is to run it as if it were already the year 2000. Running the system with dates other than the current date may require resetting the system date. There are risks involved in resetting system dates. Each organization should evaluate the impact of resetting system dates. This testing may require that your test data be "aged" properly so it contains the correct internal dates.

Hint—There are risks involved in rolling the dates on your computer systems forward. Make sure you understand what these risks are for your organization.

For some specialized systems, such as building or manufacturing control systems, or systems with embedded microchips, you may need to have the vendor work with your staff to test and assess the system.

Once you have determined the state of readiness for each system and component listed in your inventory, you should develop a strategy for dealing with those systems that have to be fixed. There are only three possible strategies: repair, replace, or retire the system.

If you decide to repair a system, there are two possible repair strategies or approaches: windowing or date expansion. The date expansion strategy involves expanding all 2-digit year fields in your system's data files and in the programs that process those files so they can hold the century as well as the 2-digit year. For example, a 2-digit year field YY might be expanded to a 4-digit CCYY field, where CC is the century. The date expansion may involve increasing the size of files that hold your data.

The windowing approach involves inserting logic into your programs that interprets year fields to determine what century the year falls into before the date field is used in calculations, comparisons or sorting. An example of this logic: if the year is between 00 and 49, the century is 20, otherwise the century is 19. This is called the 50 year window. There are other windows. You need to determine which one is appropriate for your particular system. Whatever windowing logic is selected, we recommend consistency throughout your organization to avoid later errors and confusion.

Most businesses are taking a mixed approach, fixing some systems using windowing logic and others with date expansion. Some are using such a mixed approach to fix even large systems. Your choice depends on your own individual needs.

If your strategy is to replace a non-ready system, you have several choices. You can build the replacement in-house (or hire contractors to work with your staff to build it), you can purchase a replacement system from a vendor, or you can outsource that particular line of business to a service bureau or other outside service provider. It is very important to determine when the replacement will be ready. If the replacement won't be tested and installed until after the “time horizon to failure,” you may be forced into a repair strategy.

A business system that operates in isolation is very rare. Most interface with other business systems to exchange data, and some interface with systems outside your organization. Your strategy to replace or repair non-ready systems should take into account those systems' interfaces with other systems, both within and outside your organization. For example, if you opt for date expansion, you must consider the impact of sending larger files to all interfaces. If you opt for windowing, all interfaces must be informed what the windowing scheme is.

Hint—We recommend that you develop a chart that shows the systems that have interfaces, what those interfaces are, and when they occur.

Different systems that interface with each other may have different schedules for assessment, correction, and implementation. It may be necessary to build “bridges” between systems that are ready for the year 2000 and those that are not. These bridges, which are usually temporary programs, take data from one system and modify it to make the format correct for the interfacing system. Careful, detailed planning will be required to handle these situations.

When you find that a system is not year 2000 ready, determine how critical that system is to your business. For example, if the system prints an invalid date on an internally used report, you may decide that this problem is not significant enough to address. If, however, the system loses track of inventory data or fails to forecast properly, it should be fixed.

Hint—As you purchase new computers, packages, and other hardware, upgrade existing packages, and develop new lines of business, remember that this new equipment needs to be checked to ensure it is year 2000 ready. Upgraded packages also need to be checked for readiness after upgrading.

(4) Correction and Testing—implementing the readiness strategy you have chosen and testing the fix

Testing is a critical aspect of any year 2000 project. Testing verifies that the repaired or replaced system operates properly when the date changes and that existing business functions (such as accounting, inventory control, and order tracking) continue to operate as expected. Testing also verifies that interfacing systems are not adversely affected. You should not confine your testing efforts solely to computer programs. Other systems (including network operating systems, vendor-supplied software, building infrastructure systems, PCs, and components with embedded microchips) should be tested to ensure they will not fail when the century changes.

There are several critical tests you should perform once you've changed or replaced a system. The best way to see if a system is ready for the year 2000 is to test the system as if it were already the year 2000. Test that the system will operate correctly after the date has rolled over from 12/31/1999 to 1/1/2000. Because the year 2000 is a leap year, you should test that your system will recognize 2/29/2000 as a valid date and that it will roll over from 2/28/2000 to 2/29/2000, and from 2/29/2000 to 3/1/2000. You should also test your fixed system with a date before 2000 to insure that it works. See the attachment for other suggested dates to test on your system.

Warning—There are risks involved in rolling dates forward on computers. Some computer security systems keep track of the last time a user accessed a system and will revoke or inactivate that user's password if it has not accessed the system for a period of time. Rolling the date forward may cause user passwords to be inactivated by the security system.

Datasets that should be retained may be marked as expired and could be written over. Some software packages may be leased and you may be paying an annual fee to the vendor. Rolling the date past the end of the lease may cause the software package to freeze up or generate error messages.

There are several other tests that you may want to carry out, depending on the functions your system supports. If your system does end-of-week, end-of-month, end-of-quarter and/or end-of-year processing, these should be tested. You should test that the system will forecast and retrieve data properly. Set the date to a date in 1999 and check that the system will forecast into the next century. Set the system to a date in the 21st century (any date after 12/31/1999) and test that the system will retrieve historical data from some period before 12/31/1999.

Hint—Whenever possible, testing should be carried out in a test environment to minimize the chance of corrupting the production systems. Also, be careful changing historical or backup files if you choose date expansion. You may lose an important audit trail. We suggest you consult with your auditors and legal staff before changing historical or backup files.

Definition—The term "production environment" refers to the set of hardware and software that supports your day-by-day operations. "Test environment" refers to the hardware and software where new or changed systems can be tested without disturbing your day-to-day operations.

Hint—Testing of changed systems should be carried out in an environment that is ready for the year 2000. You should work with your vendors to determine when their hardware platforms will be compliant and use those dates to build your test plans. If your vendor cannot supply the platform in time to meet your schedule, you should be aware of the risks involved and be prepared to retest your changed systems once the platform is ready.

(5) Implementation—moving your repaired or replaced system into your production environment

Before you install your replacement or repaired system, you should develop an installation plan and contingency plans. The installation plan lists all the files and programs that need to be moved into production, and all the steps to make your changed system work. Your installation plan may include testing in production to insure that the installed systems are working as expected. Contingency plans list the possible problems that you can foresee and what steps you will take if these problems occur.

Hint—You may want to make backups of the production files from the old system. If possible, you may want to install the ready system and run it in parallel with the old system and compare results.

Reminder—Your contingency plans should not include reverting to the old system. The old system is not ready for the year 2000, otherwise you would not be replacing or repairing it.

Warning—In planning to replace a system, make certain that you allow enough time to replace all of the necessary pieces of that system.

DON'T GET CONTAMINATED

Once you have repaired your systems and made them year 2000 compliant, you should take steps to make sure that subsequent changes do not contaminate those systems with year 2000 bugs. A system might get contaminated if a programmer makes changes to a repaired system and inadvertently changes the logic that handles the century change. A vendor-supplied package might also become contaminated if subsequent releases of the package don't include the year 2000 changes.

Retest the year 2000 changes as part of any subsequent system modification effort. We recommend that you save the test data and test cases that were used to test the original changes and use them whenever you are testing other changes to that system. This is called regression testing. We also suggest that any new releases of vendor-supplied packages also be year 2000 tested.

PERSONAL COMPUTERS

Today personal computers are widely used in many businesses. All personal computers have an internal clock/calendar that maintains and reports the date and time. In some computers, the year is stored and processed as two rather than four digits. The year 2000 will affect these computers just as it affects other systems. If you are running systems on your computers that access that PC's date, these systems may fail or produce bad results. All PCs should be tested, regardless of how they are used.

An insert in this brochure lists the steps you can follow to test your personal computer. You can also run PC test software that is available on the Internet.

Take an organized approach to this problem. List all your PC's, test them for readiness, and mark those that are not ready for later attention. Bright fluorescent labels can be used to mark PCs as ready or not.

There are several possible ways to correct this PC date problem. You may contact a computer retailer to investigate purchasing a new Basic Input/Output System (BIOS) chip that is year 2000 ready, download software solutions from the Internet, or replace the non-ready PC with a model that is.

Hint—Anytime you reset the date on a PC, you run the risk of corrupting your system. You can minimize that risk either by backing up all of the critical files or by resetting the date in a test environment. Don't forget to reset the date to the correct date/time after you have tested the system. If you are testing a LAN file server, power off all of the workstations connected to that LAN before going through the date test procedure.

Warning—Even a brand-new state-of-the-art PC may not be ready for the year 2000. New PC's should be tested before they are installed.

YOUR BUSINESS IS NOT ALONE

No business exists in a vacuum. Yours is part of a chain of customers, suppliers, utilities, and vendors. Year 2000 failures in any of these can impact your business. Here are some tips to protect your business within this chain.

Vendor-supplied products—Many software vendors were caught by surprise by the year 2000 problem and some will not be able to make their products ready. Others may make their products ready but may not be able to deliver the ready software until late 1999. Some vendors may no longer support a particular product that you may be running, and other vendors may have gone out of business.

For date-sensitive systems, contact the vendors to find out their readiness plans. If a vendor will not give you information about the readiness status of a package, or if a ready version will not be available until late in 1999, you should investigate an alternate system. Even if a vendor insists its product can handle the century date change, you still should test and certify it to your satisfaction. If the vendor insists that an upgraded version of a program package is ready, that package still must be tested since the vendor may have a different definition of readiness.

Data processing service bureaus—If you use a service bureau for your data processing needs, contact it to discuss its plans for year 2000 readiness.

Make a list of all the services provided by your service bureau, ranking them according to how critical they are to your business, and then contact the service bureau in writing about each service. If a service bureau says it is ready for the year 2000, ask it to provide test results demonstrating this. If possible, test the service for yourself. If it is ready for certain services but not for others, you should determine what this means to your business. Decide if there is a "work around" you can implement. If the service bureau says it will have a year 2000 version in the future, you need to assess what that means to your business. A date late in 1999 may be too risky.

Utilities and services—If your local utility fails to provide you with water, gas, or electricity, your buildings will not be usable and your business will suffer. You should also contact other companies that provide essential services such as janitorial, repair, delivery, etc. You should contact all of your suppliers to discuss the state of their year 2000 readiness and make contingency plans.

Record storage/retention firms—You may use such a firm to store critical legal documents and backup tapes offsite. These firms should be contacted to determine their state of readiness. It could be disastrous if you have an emergency and discover that your offsite storage firm can't find your backups.

OTHER SOURCES OF HELP

There are many helpful sources you can turn to for making your business ready for the century date change. The Internet has thousands of web sites dedicated to the year 2000 problem. Many sites have links to sources of freeware, planning tools, discussion groups, and so forth.

Here is a short list of useful Web sites.

http://www.year2000.com—Peter de Jager's Web site—a good source of links to other sites

http://www.compinfo.co.uk/y2k/manufpos.htm—contains links to computer manufacturer's home pages where you can find Year 2000 compliance information

http://www.software.ibm.com/year2000/—IBM's Year 2000 page

http://www.microsoft.com/smallbiz/edge/yr2000/default.htm—Microsoft's Year 2000 page

http://www.gmt–2000.com/gmt–2000/homepage—frameset.html—the link to Greenwich Mean Time's home page with evaluations of PC testers and BIOS chips—useful for PC evaluation

http://pw2.netcom.com/helliott/00.htm—The so-called "Mother of all Y2K link sites" contains many links to other sites

http://www.jks.co.uk/y2ki/confer/notices/dtisme01.htm—link to a report "Helping the Small Business Tackle Year 2000"

http://www.isquare.com/y2k.htm—The Small Business Advisor Web site

http://www.bog.frb.fed.us/y2k/—The Year 2000 page of the Board of Governors of the Federal Reserve Bank

http://www.ffiec.gov/y2k/—The Year 2000 page of the Federal Financial Institutions Examination Council

http://www.frbsf.org/fiservices/cdc—The Federal Reserve Bank of San Francisco's year 2000 page

Professional organizations or trade associations may be able to provide you with support and advice. There are many consulting firms and independent consultants who can help you get your business ready for the century date change. Many data processing and business magazines have articles about the year 2000 problem and most large cities now have year 2000 user groups that meet to discuss the problem. One magazine that is dedicated solely to the year 2000 problem is called The Year 2000 Journal. The Journal can be reached at (214)–340–2147; its Internet address is http://www.y2kjournal.com.

If you can't find a year 2000 user group in your area, form one. It can become your support group and someone in your group may have already solved problems that you are facing. If you form, or join, a year 2000 user group, invite local political officials to become involved. They will have to work with their local government agencies to ensure that police and fire services, water, electricity, and other utilities are uninterrupted.

SOME QUESTIONS TO HELP ASSESS SYSTEM READINESS

1. Can the system perform projections through time? For example, can it calculate interest or payments or make inventory projections?
2. Does the system allow for entering dates? If yes, is the year 2 or 4 digits? What happens if you enter "00" or "01?"
3. Will the system operate differently depending on the day of the week? Will it operate differently at month-end, quarter-end, or year-end?
4. Can the system put things in order by date?
5. Does the system allow you to retrieve things by date?
6. Can the system perform date-based calculations?
7. Does the system have a security feature that includes date checking?

SUGGESTED TESTING CRITERIA

The following list is not all inclusive. You should add others based on your business's needs and ignore those that are not appropriate.

1. Test the changed system with dates before the year 2000 to insure that it is working properly.
2. Test that the changed system rolls over from 12/31/1999 to 1/1/2000 properly.
3. Validate the first business day of the year 2000 (1/1/2000, 1/2/2000 or 1/3/2000 depending on your business needs).

4. Validate that the system operates correctly at end-of-month (1/31/2000 and will roll over to 2/1/2000 properly.
5. Test that the system rolls over from 2/28/2000 to 2/29/2000 properly, operates correctly on 2/29/2000, then rolls over and operates properly on 3/1/2000.
6. Test 3/31/2000 and 4/1/2000 to show that end-of-quarter processing operates correctly.
7. Test 1/7/2000 and 1/10/2000 to insure that the system operates correctly on the first Friday of the new century, and on the Monday after the first Friday.
8. Validate year display fields, including data entry.
9. Validate the year in reports.
10. Test that the system sorts in correct order, validate all sort processing.
11. Validate correct calculation of dates.
12. Validate the correct acceptance of dates from the operating systems.
13. Validate calculated resultant values from dates.
14. Test that ages are calculated correctly.
15. Validate interest and other time-based financial calculations.
16. Test expiration date processing.
17. Test historical decision analysis.
18. Validate time reporting processing.
19. Test workflow/materials requisition and inventory processing.
20. Verify that billing calculations are correct.
21. Validate cycle processing, including day-of-week and/or first business day of the month.
22. Verify that the system forecasts correctly.
23. Test forward processing—process dates after the year 2000 (2001, 2002, &c.).
24. Validate backward processing—process dates prior to 2000.
25. Verify historical or archival date processing.
26. Validate that the system purges the correct records.
27. Validate date and data error handling routines.
28. Validate date expansion, if used, both within the application and between interfacing applications.
29. Validate windowing, if used, both within the system and between interfacing systems.
30. Validate proper handling of special values in dates—99/99/9999, 88/88/8888, 00/00/000.
31. Validate that the system works with the date 1/1/1999—first date with "99" in the year field.
32. Validate that there are 366 days in the year 2000, and 365 days in the year 2001.
33. Validate that 9/9/99 (September 9th, 1999) is handled properly.

Some additional dates that may impact businesses.

1. 7/1/1999—46 out of 50 states start their fiscal year 2000.
2. 10/1/1999—start of Federal Government's fiscal year 2000.
3. 2/15/2000—W2 due.
4. 4/15/2000—Tax day.
5. 4/30/2000—first month ending on a weekend.
6. 5/1/2000—tax withholding report due, unemployment tax due.
7. 9/30/2000—Federal Government's end of fiscal year 2000.
8. 10/10/2000—first "6-digit" date for systems storing date as MDDYY.
9. 12/31/2000 (Sunday)—first year end—check that year contains 366 days.
10. 1/1/2001—test that the system has been instructed to roll over to 2001.
11. 2/29/2001—invalid date.
12. 12/31/2001—second year end—check that year had 365 days.

HOW TO CHECK A PERSONAL COMPUTER FOR YEAR 2000 READINESS

The following steps are suggested to determine if a personal computer will roll over to the year 2000 correctly.

The test presented here requires a bootable DOS floppy diskette. This is a safer method to test your PC's system clock because it leaves the data and programs on your PC's hard disk unaffected. If you boot to your C: drive, you may end up loading Windows or Windows 95 and other applications from your startup routine. Using a bootable diskette will ensure the integrity of the data and programs on your PC's hard disks. The test script presented here will check your PC's ability to transition to the year 2000 and recognize it as a leap year.

Do not perform the tests by changing your system's BIOS Setup screen.

Create a bootable test diskette. Insert a blank floppy diskette into the PC's A: drive. From a DOS prompt, type FORMAT A: /S. Or from Windows File Manager, click on DISK/FORMAT and check MAKE SYSTEM DISK.

With the bootable diskette created in Step 1 still in your PC's floppy drive, shut down your system (close Windows) and the power off your PC. Don't just hit the reset button or warmboot (CTL-ALT-DEL).

Turn the power on your PC, and allow the PC to boot from the diskette.

After bootup, DOS automatically shows the current date. Make sure that the correct date is displayed. Otherwise, you may have to set the correct date on your PC's BIOS.

At the Enter new date (mm-dd-yy) prompt, type 12–31–1999.

After changing the date, the current time will be displayed.

At the Enter new time: prompt, type 23:55:00.

Turn the power off on your PC and wait at least 10 minutes. If you don't, DOS will appear to transition correctly to the year 2000. However, once you reboot the PC, it will display the incorrect date if your system's RTC has the flaw described above.

Turn the power back on and wait for the boot process to complete.

Type in Date at the ready prompt. If Sat 01–01–2000 is displayed, your PC's BIOS passes the test.

At the Enter new date (mm-dd-yy): prompt, type 02–28–2000.

This will test your system's ability to recognize the year 2000 as a leap year.

After changing the date, the current time will be displayed.

At the Enter new time: prompt, type 23:55:00.

Power off your PC again and wait at least 10 minutes.

Turn the power on the PC. Type in Date at the Ready prompt.

If Tue 02–29–2000 is displayed, your PC's BIOS passes the leap year test.

To conclude testing, at the Enter new date (mm-dd-yy): prompt, enter the correct date, e.g., 07–04–1997.

After changing the date, the current time will be displayed. At the Enter new time: prompt, type correct time, e.g., 06:00:00.

Remove the bootable diskette from the floppy and power off your PC.

RESPONSES OF FRED P. HOCHBERG TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. I understand that SBA will be guaranteeing 50 percent of the loan value up to $50,000 to help small businesses pay for Y2K fixes. Can you characterize or project how quickly the guaranteed funding will enable small businesses to complete remediation and testing efforts? For example, if a typical small business were to obtain funding and begin remediation efforts in December of 1998, what are the chances they could reach compliance by the year 2000?

Answer. The legislation (H.R. 3412) establishing a targeted Y2K pilot loan program at SBA failed to pass before Congress adjourned. However, SBA believes its current loan programs are already structured to do the type of Y2K mitigation loans envisioned in this legislation. SBA recently changed its SBAEXPRESS and LowDoc programs to expedite and simplify the delivery of funds to small businesses. These programs are specifically designed for the type of loans that businesses would need to address Y2K in an expedited manner. For example, under our SBAEXPRESS program, small businesses can receive a loan to address Y2K-related problems for up to $150,000 with a guaranteed turnaround time of 36 hours or less.

With regard to the second question, the time required for Y2K remediation efforts will vary from one small business to the next depending upon the complexity of the Y2K issues at each small business. If the fix happens to be solely reprogramming the internal clock of a personal computer, then obviously the fix can be done quickly, often within one day. If the fix involves a complete overhaul of entire systems, including procuring new machines, then the fix will be more complex and may take anywhere from a week to many months. If the fix is reviewing computer programs, on a line-by-line basis involving millions of line of computer code, the fix may be especially long and may be dependent upon finding capable technical staff to complete the work. In this latter case, this work will require many months. Our message to all small businesses is to take action now, don't delay. To assist small businesses in getting quick access to the information they need, SBA's Y2K website (www.sba.gov/y2k) we have include direct links to over sixty computer hardware and software manufacturers.

Question 2. What sort of figures or data can SBA provide about the potential impact of small business failure on the supply chain? For example, if it is expected that 50 percent of all business experience a failure of a mission critical system, does SBA have any projections as to how this could impact the economy in either the short term or long term?

Answer. The SBA does not have any data regarding the impact on the economy in either the short term or long term as a result of the Y2K issue and possible small business failures. However, we do believe that the Y2K issue is a management issue, not a technical issue. As such, small businesses who exercise prudent management judgement in their everyday operations will successfully solve their Y2K issues in a timely fashion. Those small businesses that are unable to address ongoing management challenges will also have a difficult time in addressing the Y2K issue. In other words, I believe few small businesses will fail solely because of the Y2K issue. A small business with poor management skills is likely to fail because Y2K is just one of many issues they have not been able to overcome. Accordingly, the success/failure rate of small businesses will not be radically affected and the overall effect on the economy will be minimal.

Question 3. What is the greatest concern SBA has for small businesses?

Answer. Our greatest concern is that small businesses are not taking action soon enough on this important issue. Small businesses tend to focus on the "here and now" as they grapple with business management issues every day. January 2000 is over a year a way and that is an eternity for most small businesses. The longer a small firm waits, the more costly the Y2K "fix" will be. Our slogan is "Its too late to start early."

Question 4. How is the SBA stressing the importance of business continuity planning? Have you identified best practices for business continuity planning?

Answer. SBA has identified best practices and developed materials, classes, seminars, speeches and a web site stressing the importance of contingency planning as part of an overall Y2K strategy for every small business. On our web site, www.sba.gov/Y2K, we offer advice on contingency planning. Specifically, we offer information on contingency planning in our seminar materials. These materials, developed by IBM for our use during our national Y2K Action Week, provide an excellent guide for small businesses as they address their Y2K issues.

Question 5. Does SBA have any estimates as to the overall cost of Y2K for small business?

Answer. We have not conducted any independent studies of the overall cost for small businesses. However, we are in contact with the National Federation of Independent Businesses (NFIB) and its Y2K staff. NFIB issued a study this past May on the preparedness of the small business community for the Y2K problem. It is conducting a follow-up study, which should be available by the end of this year, and has offered us the opportunity to review the data they receive. We expect the study to address this issue and give us insight on the overall cost.

Question 6. Does SBA have any figures indicating the reliance of small business on information technology? For example, do you know what percentage of small start-up businesses rely heavily on computers.

Answer. SBA has not done any research in this area and does not have any data readily available to make an estimate regarding the percentage of small start-up businesses that rely heavily on computers. In addition, we are not aware of any similar studies having been done in the private sector.

[United States Small Business Administration—Small Business Research Summary—RS Number 156 (November 1995) ISSN 1076–8904]

The Effect of Computer Use on the Earnings of Workers by Firm Size

[By Rakesh Kochhar, 1994, 104p. Completed by Joel Popkin and Co., 1101 Vermont Ave.N.W., Washington, DC 20005, under contract no. SBA–8033–OA–93]

PURPOSE

The use of computers by workers is an important element in the currentt employment shift toward higher-skill jobs. The extent of smalll businesses' participation in this shift, and the wage benefitss by firm size to employees participating in the shift, are thee subjects of investigation in this study.

Many policy-makers believe that the competitive potential of U.S.businesses—both at home and abroad—will depend on the ability off firms to incorporate computer-based technologies and to upgrade thee skills of their workers. It is important to understand how smalll and large firms have adapted their work places to the emergingg information-based economy and whether they have realized similarr gains in productivity from the use of computers. Productivity gains from the use of computers is expected to be bestt measured by the wage differential of computer users over otherr workers in the same industry.

SCOPE AND METHODOLOGY

Data for this research became available with the inclusion of a question on computer use in the Current Population Survey (CPS) of January 1991. These data were merged with data on firm size from thee March 1991 survey and wage data from the April 1991 survey.The CPS is a regular survey of households by the Bureau of the Census and covers over 50,000 households. The survey panel changes fromm month to month, so only those households included in the surveyy in all three periods could be used. The result was 28,407 observations that matched across all three time periods, or less thann half of the 67,374 individuals reporting on employment in January 1991. Workers under the age of 16 and over the age of 65 were eliminated from the sample, as well as a few workers with very low wages. The final sample was 18,009 individuals. The data permitted further analysis by worker age, education, sex,job tenure, industry, and occupation. The analysis revealed the wage returns to computer usage to be robust and nearly constant acrosss firm sizes, industries, and all of the above worker characteristics. Computer usage in information-based industries was the highest; production occupations showed the lowest computer usage by workers. Growth industries were analyzed separately and revealedd higher computer usage among workers in growing industries.

HIGHLIGHTS

—Small firms were found to be hiring college-educated workers and creating jobs at the top end of the wage spectrum in greater proportionss than in the past. Among new hires, small firms employed 58.9 percent of all workers and 54.8 percent of new hires in the top wage quartile. In the time period covered in the report, small firms were responsible for the majority of new hiring at the high end of the wage spectrum. The author states, "Between 1990 and 1991 most high-wage jobs were being created by smalll firms."

—Computer usage was twice as high among employees in the highest wage quartile compared with those in the lowest quartile. This relationship held for all firm sizes and lengths of job tenure. The overall average was 29.6 percent of workers using computers in the lowest wage quartile and 74.2 percent using computers in the highest wage quartile. The wage return to computer usage was present even among new hires in the under 25-employee firm, where the lowest wage quartile showed 21.6 percent of workers using computers and the highest wage quartile showed 58 percent using computers. To the extent that wage is based on the marginal value of worker product, computers are an important influence for higher workerr productivity in firms of all sizes.

—The highest premium for computer users over nonusers was found to be in small firms in industries with the highest growth rate, where a premium of nearly 24.8 percent in wages was observed. Fast-growing large firms did nearly as well, with an estimated 23.8-percent wage premium for computer users.

—Computer usage was highest in fast-growing firms of more than 1,000 employees, with 69 percent of employees using computers; it was lowest in slow growth firms with fewer than 25 employees where less than 31 percent used computers in their occupation. The author suggests that the 25-employee level may be a threshold for the adoption of computer technologies.

—Occupations requiring information processing exhibit computer usage four times as high as occupations that are mostly production-oriented. Information-processing occupations show computer usage to be 71.9 percent for small firms and 81.3 percent for large firms.

—Women use computers at a higher rate than men in firms of all sizes. More than 50 percent of women in small firms use computers on the job; the rate for men is below 40 percent.

ORDERING INFORMATION

The complete report is available from:

National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
(703) 487–4650
TDD: (703) 487–4639
Order number: PB95–239984

Price codes: A06 (paper); A02 (microfiche)

PREPARED STATEMENT OF SENATOR JON KYL

Small and medium size businesses are key elements in the robust American economy. Experts have projected that a good number of small and medium-sized business may very well fail because of the Year 2000 computer problem. In fact some recent news articles across the country are citing projections that up to 12 percent of small business employing 50 people or less may be expected to declare bankruptcy. What would happen if 12 percent of the small businesses in the U.S. were to fail in the first quarter of 2000? How do we ensure that the supply chain necessary for commerce and defense remains unbroken? Making sure that small and medium sized business are prepared and have the resources they need is an important step.

The good news is that a small business can often fix their problems faster; the bad news is that small businesses often do not have the "in-house" technical expertise or budgets to fix Y2K problems. The Passage of the "Year 2000 Information Disclosure Act" (S. 2392) and the Year 2000 Readiness and Small Business Restructuring Act of 1998 (H.R. 3412) provide important resources for the business community. S. 2392 helps increase the flow of technical information needed for identifying and correcting problems, and H.R. 3412 helps ensure that small business can borrow the funds they to finance Y2K fixes.

According to Frank Zarb, the chairman of the National Association of Securities Dealers, parent of the Nasdaq stock market, "I believe we're in good shape but I'm still worried. We know, like everyone else does that there are going to be some crises, so we formed crisis teams that can parachute in after that day." I appreciate Mr. Zarb's well balanced approach. I think this represents a realistic model for small and medium sized businesses. Know your vulnerabilities, do everything you can to prepare for Y2K and do not neglect your business continuity plans.

It is in the best interest of every business to investigate their Y2K vulnerabilities and build the necessary business continuity plans. Small and medium sized businesses are the biggest employers in the country, and it is essential that they make the transition to the next century in a well executed fashion. Mr. Chairman, I look forward to today's hearing.

PREPARED STATEMENT OF KEITH MALLONEE

Mr. Chairman and distinguished members of the committee: I am pleased to appear today before the Special Committee on the Year 2000 Technology Problem. My name is Keith Mallonee. I am the vice president of systems development for McKesson Corporation. In keeping with the Committee's request, I will provide a brief overview of McKesson's program to address the Year 2000 or 19Y2K' issue and respectfully request that my full written statement be included in the record of this hearing.

McKesson is the largest national distributor of pharmaceuticals, health care products, medical and surgical supplies, with sales in excess of $20 billion for our current fiscal year. Our customers are located in all 50 states, and include hospitals, independent pharmacies, chain drug stores, food stores, clinics, nursing homes, government facilities, physician groups, HMO's and surgical centers.

Today I am here to share with you the importance of electronic commerce to our company, the preparations McKesson is making for Year 2000 and the state of our developing contingency plans.

Electronic commerce is very important to the success of our business and the business of our customers. McKesson supplies pharmaceuticals and health care products to roughly 35,000 customers and processes about 60,000 orders containing 1.6 million order lines daily. Virtually all of these orders are sent to us by customers in some electronic form or another using everything from small hand held electronic devices that connect to phones to large mainframe computers. In addition, all major movements of funds including customer remittances and payroll are handled electronically through electronic fund transfers.

On the inventory management side of our business, we are equally dependent on electronic commerce. Roughly 80 percent of all trade goods purchased by McKesson are ordered through electronic data interchange, or EDI. Payments to our larger trade suppliers are also handled through EDI with commercial bank payment services.

McKesson has become very dependent on electronic commerce and we are taking great care to ensure the efficient functioning of this environment continues with minimal interruption as we enter the new millennium.

How has McKesson prepared for the Year 2000? Just as we would any other major project. In 1996, we began with a survey of all of our operations to get a better appreciation for the scope and skills required. We then created a Year 2000 central project office for which I am responsible. In 1997, we began developing corporate-wide standards, dividing the problem into manageable projects, then developing plans and budgets.

Today we are finalizing software and hardware changes and testing the integrity of these changes extensively. We monitor our progress across the enterprise through reports submitted on a regular basis to our central project office, our Chief Information Officer, an executive steering committee and ultimately to McKesson's Board of Directors. McKesson's Internal Audit Department has independent staff members conducting company-wide reviews of subsidiary and divisional Year 2000 efforts. The results of these reviews are presented to the Audit Committee of McKesson's Board of Directors.

McKesson's executive management has identified Year 2000 as a top corporate priority. To that end, we have an estimated 400 people, including project managers, technicians, consultants, contractors and business partners working on the problem and we expect to spend between $30–40 million in making our systems ready.

How are we progressing? A recent review by our financial auditors, Deloitte and Touche, found our progress and methods to be 'best of class', of which we are quite proud. As with any project of this magnitude and complexity, there are challenges, but at this point, McKesson does not foresee any serious obstacles meeting its Year 2000 requirements. In general, McKesson plans to complete the final system changes required for Year 2000 compliance by June 1999.

While McKesson has moved at a very fast pace to solve Year 2000 problems internally, our ultimate success is very dependent on others, particularly our trading partners and the telecommunications, electric utilities and transportation industries. As a result, contingency planning, while a normal part of our business, will become even more important as we approach the Year 2000. In the sales area, we will be capable of taking limited emergency orders manually and have provided virtually all customers with highly reliable hand held order entry devices to use in case their own systems fail. In our major data center, we have a diesel generator sufficient for normal operations with alternative telecommunication pathways and we can reroute inbound electronic orders to off-site systems. At the distribution centers we are prepared to pick emergency orders manually and ship product by any one of six modes. We have identified our most critical products and expect to have at least 45 days of supply on hand at the turn of the millennium. In addition, we are working to certify the readiness of our 2,000 inventory suppliers, with special attention to all manufacturers of pharmaceutical products.

McKesson has been in business since 1833. In the intervening 165 years, we have faced many challenges in supplying our customers the product they need within the timeframe they require. As an example, Hurricane Georges recently closed down one of our 36 distribution centers for 5 days. Similarly, we have encountered fires, floods, earthquakes, tornadoes, blizzards...and yes, even computer system failures. Even in the worst disaster McKesson has taken pride in being able to overcome the obstacles and deliver product when and where it is needed. With Hurricane Georges we quickly rerouted critical orders to two other distribution centers and continued to deliver without a serious disruption to our customers. Year 2000 is just another challenge and we will meet it just as we always have.....our customers have grown to expect that from McKesson.

Mr. Chairman, we appreciate the opportunity to appear before the Committee today. These are critical issues facing our industry and we welcome your leadership in addressing them. I will be happy to respond to any questions that members of the Committee have, either now, or in writing following the hearing.

Response of Keith Mallonee to Questions Submitted by Chairman Bennett

Question. How is McKesson avoiding the generic problems of IT interconnectivity both domestically and foreign with its EDI trading partners?

Answer. Almost all of McKesson's 35,000 customers are using McKesson-owned portable order entry devices that support both manual key entry or bar-scanned entry. These units are Year 2000 tested, are not dependent on EDI technology except for a working phone line, and have been in use by McKesson customers as a sole or alternative order entry device since the late 1960's.

McKesson also offers customers an opportunity to transmit limited orders via any touch tone phone.

If we have a Year 2000 problem with our telephone carrier, we can, to a certain degree, use alternate lines, hubs and carriers. At this point McKesson expects that if there are telephone problems, they will be local, if at all.

Electronic fund transfers, normally accomplished through EDI, can be accomplished by simple wire transfer.

To limit the chance of Year 2000 EDI problems, all EDI trading partners have or will receive an invitation to participate in test EDI transmissions as a part of our Year 2000 effort.

There are ready alternatives to EDI. For example, orders with EDI suppliers can be faxed, telephoned, FedEx'd, or even delivered by regular mail.

In addition, McKesson has no suppliers using EDI with ordering points outside the United States for its core business of domestic drug and healthcare distribution.

Question. To what extent is McKesson dependent on foreign suppliers and how do you expect to avoid the Year 2000 problem with them?

Answer. Our core business (domestic wholesale healthcare distribution) purchases very little, if any, directly from foreign suppliers and any such transactions would be handled by non-electronic means (such as mail or fax). We do not, therefore, anticipate a direct Year 2000 issue with foreign suppliers for our domestic wholesale healthcare distribution business. It is difficult to fully evaluate our indirect exposure where, perhaps, McKesson deals with a company that purchases raw or finished goods from outside the United States.

Our foreign subsidiary, Medis in Canada, also purchases exclusively within Canada. Medis is working on their own Year 2000 plan to include vendor Y2K certification. McKesson also has a minority interest in Nadro of Mexico but we have been unable to determine to what extent they purchase from foreign suppliers.

Question. To what extent have you coordinated, negotiated or otherwise contacted your suppliers and customers to make certain that they will be Year 2000 ready? Will you continue to do business with companies that are not Year 2000 ready?

Answer. A review of material relationships with suppliers of technology and trade goods was included in the McKesson Year 2000 project.

We are participating in an industry effort organized by the National Wholesale Druggists' Association (NWDA) to verify the Year 2000 readiness of trade suppliers with special attention to manufacturers of branded pharmaceutical products. The NWDA is the national trade association for pharmaceutical distributors. McKesson is dedicated to getting Year 2000 certifications from a list of suppliers identified as critical to our business; together these critical suppliers represent over 85 percent of McKesson's purchases in 1997.

Within the structure of the core project office at corporate headquarters is a team dedicated to trading partner issues. On a daily basis McKesson is communicating by phone and letter with major suppliers and exchanging information about mutual Year 2000 interests.

On the non-trade side of the business, Year 2000 compliance statements were required from all suppliers of McKesson's computer hardware and commercial software starting in early 1997. As of October 1998, 70 percent of the computer hardware and purchased software used in the core business, wholesale drug and healthcare distribution, was compliant. Non-compliant technology was or will be replaced by June 1999.

McKesson has just established a web site containing a section devoted to Year 2000 information. This web site will allow McKesson efficient and timely communication with our trading partners and the public on key Year 2000 issues. The site is divided into 3 sub-areas: general information of possible interest to everyone, an area dedicated to customer concerns, and a separate area dedicated to supplier topics.

At this point we are not aware of any supplier that has expressed serious doubt about their ability to become Year 2000 compliant. If a trade supplier is identified with serious Year 2000 problems, the decision to cease doing business with them will rest with our product and inventory managers.

Question. What infrastructure availability did you assume in planning your Year 2000 remediation and contingency plans?

Answer. Most of our customers operate on a 19just-in-time' inventory model. They assume that they can carry a minimal level of inventory because an order placed today will be filled by McKesson tomorrow. Because McKesson distributes pharmaceuticals with health sustaining, and in some cases, life dependent attributes, this dependency is taken quite seriously. As I mentioned in my verbal and written statement to the committee on October 7, 1998, McKesson has been in business since 1833 and has managed to deliver critical products despite all types of business disruptions, such as earthquakes, tornadoes, floods, fires and hurricanes. In some of those situations, distribution center phone lines have gone dead, power has failed, employees have been unable to get to work, computers have failed, and normal resupply has been disrupted. In these cases, our local managers, administrative staff, sales people and warehouse employees have picked critical orders by hand or shifted orders to other distribution centers for filling. Critical product was moved from one distribution center to another to cover short-term supplier problems, and orders were faxed rather than transmitted by EDI. You can be very resourceful if someone's health and your business relationships require it.

McKesson relies heavily on technology in its infrastructure and has moved aggressively to address both internal and external Year 2000 concerns. Because of our strong internal Year 2000 organization, we are becoming increasingly confident that, internally, our systems will successfully meet the Year 2000 challenge.

We currently believe that the most likely risks of Year 2000 business disruptions are external in nature and may occur in telecommunications, electric, or transportation services and with non-compliant smaller trading partners. Problems will probably be localized, non-critical and hopefully short in duration. The most serious disruption would be an extended and/or extensive communications failure. Such an extensive communications failure is not considered likely based on our monthly Year 2000 reviews with major communications carriers, the flexible design of our network, and our use of backup and off-site systems.

Question. How does your company rate the potential Year 2000 impact of microprocessors on your business?

Answer. Internally, McKesson uses microprocessors in desktop and laptop computers, security systems, servers, controllers, telephone equipment, time keeping and reporting devices, portable intelligent scanning equipment used in our warehouses, and in a multitude of other devices. At this time we are not aware of any internal situation where a device using a microprocessor would cause a serious impact on our business. It's difficult to evaluate the potential external impact of microprocessors on our business, but I am not aware of any serious problems.

Question. What percentage of your overall time will be spent testing as compared with time spent on remediation tasks? Will your testing phase extend beyond June of 1999?

Answer. We estimate that at least 60 percent of our total Year 2000 effort will be devoted to testing. Testing is an important part of McKesson's Year 2000 effort. All existing and modified computer code has, or will be, subjected to an extensive, well-defined, multi-tiered, series of tests. Throughout calendar year 1999 we will be conducting a rigorous final level of review called integrated testing under post-Year 2000 conditions.

Prepared Statement of Lou Marcoccio

INTRODUCTION

GartnerGroup is a worldwide business and information technology advisory company, providing research and advice in more than 80 major focus areas of business and technology, including Year 2000. We research Year 2000 status, issues, and best strategies, and provide advice and methods to companies and governments throughout the world.

Major points in this testimony:

(1) Year 2000 worldwide compliance status
(2) Predicted failures and impact
(3) The impact of embedded chips
(4) When system failures will occur throughout the duration of this problem
(5) Risks to the United States and possible impact
(6) Accuracy of disclosures reported to the U.S. SEC
(7) Recommendations to the United States Senate

Method of Measurement of Compliance Status: COMPARE (COMpliance Progress And REadiness): GartnerGroup uses a methodology for determining the status of a company or government agency. It is used to rank and compare level of completion of compliance. It consists of five levels:

(1) Level 0—Has not started any Year 2000 effort
(2) Level I—Starting, awareness, champion identified, begin business dependency inventory
(3) Level II—Conduct detailed inventory of all business dependencies

(4) Level III—Detailed project plans, resources in place, prioritize business dependencies, risk assessment, complete compliance of 20 percent critical items

(5) Level IV—Complete compliance efforts on remaining 80 percent of critical items

(6) Level V—Complete compliance of non-critical items and launch policies to guard against post year 2000 failures

RESEARCH METHODS

This information is gathered from interviews and client inquiry meetings. GartnerGroup is prohibited from disclosing specific names of companies or government agencies that are providers of this information, due to agreements of disclosure, under which the information is provided. Research data is gathered using various research methods, e.g., client interviews, surveys, consortia groups, user companies, equipment manufacturers, consulting firms, and legal firms. The research covers 15,000 companies in 87 countries. An attempt was made to equally distribute the research across small (under 2,000 employees), medium (2,000 to 20,000 employees), and large (over 20,000 employees) companies in each country, and to equally distribute across 27 vertical industries. We analyze the research and produce predictions and analysis. This information is provided to clients in our written research and advice. Year 2000 status of companies and governments has been found to be quite different in each of three dimensions—size, industry, and country.

RESEARCH RESULTS

23 percent of all companies and government agencies have not started any Year 2000 effort. 83 percent of these are small companies with fewer than 2000 employees.

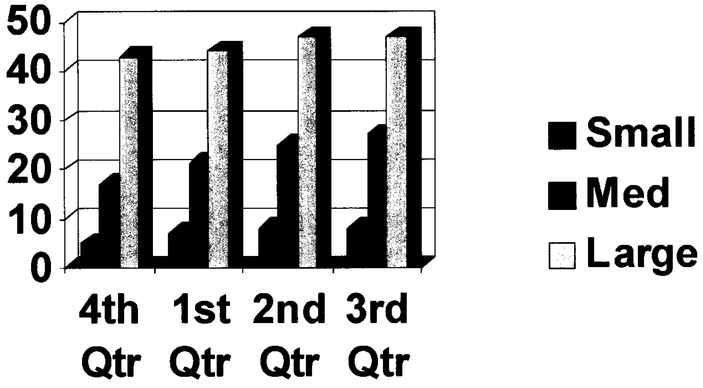


Figure 1 : *Percent of Companies With Year 2000 Projects, by Size - 1998*

Why Companies & Government Agencies Began to Address This Problem

(1) A failure occurred affecting a mission critical business process

(2) Regulatory mandate and possible penalties

(3) Fear of internal litigation due to lack of due diligence

(4) Customer pressures

Since awareness and failure scenarios have reached many countries, many companies are now getting started because of fear of interruptions to their supply chain and pressure from customers.

Characteristics by Size

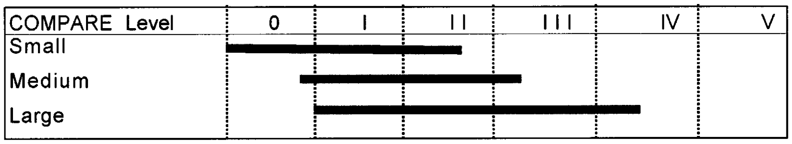


Figure 2 : *Status of Companies and Government Agencies, by Size; Q31998*

Large companies are farthest ahead. They began earlier, because failures occurred, they had more resources to deploy, and they had older systems critical to their continued business operation. They spend a larger percentage of NOR (net operating revenue) on IT (information technology) than small companies. Smaller companies have fewer resources and less resource flexibility. A large percentage of IT systems at large companies were built in-house. Small companies have purchased a much larger percentage of IT systems from vendors. Since a majority of business insurance carriers recently added Year 2000 exemptions to current active business interruption policies, companies will not be able to rely on their insurance coverage as they planned. Many large companies have cash reserves and internal insurance strategies to rely upon, whereas small companies have limited safety nets or parachutes.

As of Q3 1998, large companies have completed remediation of 20–80 percent of their internal systems, and 30–50 percent have started significant levels of testing. Mid-size companies have 0–30 percent remediated, and 20–40 percent have begun testing. Small companies have 0–5 percent remediated, 30 percent have begun testing, and they are heavily reliant upon vendors to fix their systems. Large companies are using their own internal resources and contracting only 2–7 percent to outside vendors. Mid-size companies are contracting 25 percent to vendors, while small companies are contracting 50 percent to vendors.

IT budgets were relatively flat from 1997 to 1998, however 30 percent of IT budgets will be spent on Year 2000 efforts in 1998. We estimate 44 percent of IT budgets will go to Year 2000 projects in 1999.

Small companies spend 50 percent of their Year 2000 spending on outside services, while large companies do most of the work themselves with already-existing internal resources.

From 1996 through Q1 1998, companies were using vendor form letters to determine supply chain risks. Many of these are not responded to, and of the ones received, the vast majority are unusable for compliance risk assessment. During Q1 and Q2 1998, more than 60 percent have changed to a strategy of requesting face-to-face or telephone (direct contact) vendor reviews. This should help in obtaining more accurate supply chain risk information; however, many are struggling with trying to get vendors to agree to this type of meeting. Therefore, getting vendors to disclose accurate information related to compliance of their products remains a challenging task.

Prior to 1998, 5 percent of companies had business participation or business ownership of compliance efforts in their company. During 1998, this grew to nearly 30 percent. We forecast that companies in which the IT organization "owns" the Year 2000 compliance projects for the corporation are 3–5 times more likely to have a serious mission critical system failure (0.8 probability).

The predominant focus of Year 2000 projects differ considerably, based upon the size of the company and country it is in. Large companies are now focused on contingency planning and assessing business dependency risks, while continuing to complete fixing of internal systems and beginning to test (see Figure 2). Mid-size companies are just beginning to address contingency planning, while attempting to assess supply chain risks and trying to leap-frog steps required to fix and text internal solutions (see Figure 2). Many small companies have still not started, but the ones who have, are focusing on vendor compliance and inventorying their business dependencies (see Figure 2).

In April 1997, 50 percent of companies, across all industries, had not started Year 2000 efforts. By November 1997, the number dropped to 30 percent. By October 1, 1998, 23 percent of companies throughout the world had not started. 83 percent of those are small companies. We predict that in January 2000, nearly 20 percent will still not be started, and they will mostly be small companies and companies in lagging countries (0.8 probability).

PREDICTED FAILURES BY SIZE

GartnerGroup defines a “failure” as an interruption to a business operation, a business dependency which cannot be provided or delivered as required, or inaccuracy of data or customer transaction. “Mission critical” is defined as any business dependency which, if it were to fail, would cause any of the following:

(1) A shutdown of business, production, or product delivery operations
(2) Health hazard to individuals
(3) Considerable revenue loss
(4) A significant litigation expense or loss
(5) Significant loss of customers or revenue

30–50 percent of companies and government agencies worldwide will experience at least one mission critical system failure (includes all sizes, all industries, all countries) through Q1 2000. In the U.S., 15 percent of companies and government agencies will experience a mission critical system failure (also see section on country status for status of U.S. versus all other countries). 10 percent of failures will last 3 days or longer. The cost of recovering from a single failure after it occurs will range from US $20,000—$3.5 million.

The number of companies predicted to experience at least one mission critical system failure (0.8 probability):

—50–60 percent of *small* companies and government agencies
—40–50 percent of *mid-size* companies and government agencies
—10–20 percent of *large* companies

CHARACTERISTICS BY INDUSTRY SECTOR

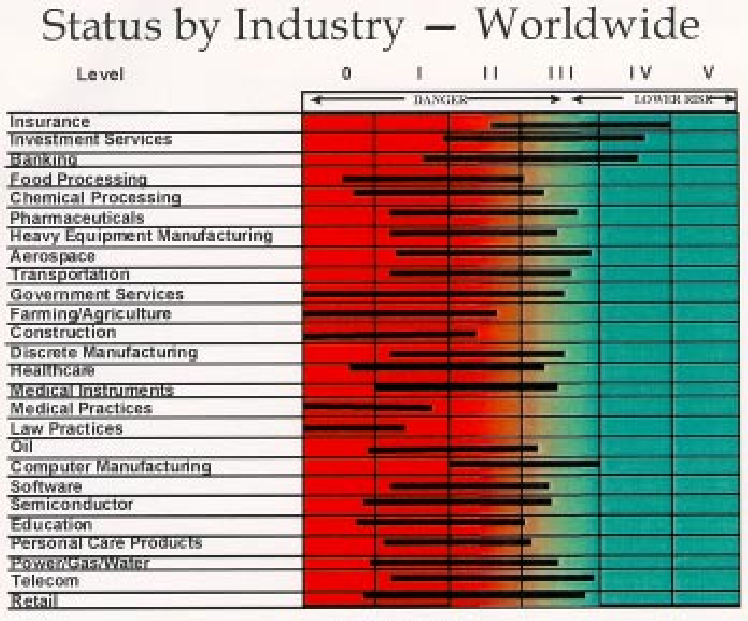
The second dimension used to gather Year 2000 status information is by industry. We monitor 27 industries, and find there are distinct issues unique to each industry. Very few of the industries are regulated. The industries have been placed into four risk categories.

Figure 3 : ***Research Industries and Failure Predictions***

Category 1.—Insurance, Investment Services, Banking, Pharmaceuticals, Computer Manufacturing.	***15 percent*** of companies in these industries will experience at least one mission critical system failure.
Category 2.—Heavy Equipment, Aerospace, Medical Equipment, Software, Semiconductor, Telecom, Retail, Discrete Manufacturing, Publishing, Biotechnology, Consulting.	***33 percent*** of companies in these industries will experience at least one mission critical system failure.
Category 3.—Chemical Processing, Transportation, Power, Natural Gas, Water, Oil, Law Practices, Medical Practices, Construction, Transportation, Pulp & Paper, Ocean Shipping, Hospitality, Broadcast News, Television, Law Enforcement	***50 percent*** of companies in these industries will experience at least one mission critical system failure.
Category 4.—Education, Healthcare, Government Agencies, Farming & Agriculture, Food Processing, City & Town Municipal Services	***66 percent*** of companies in these industries will experience at least one mission critical system failure.

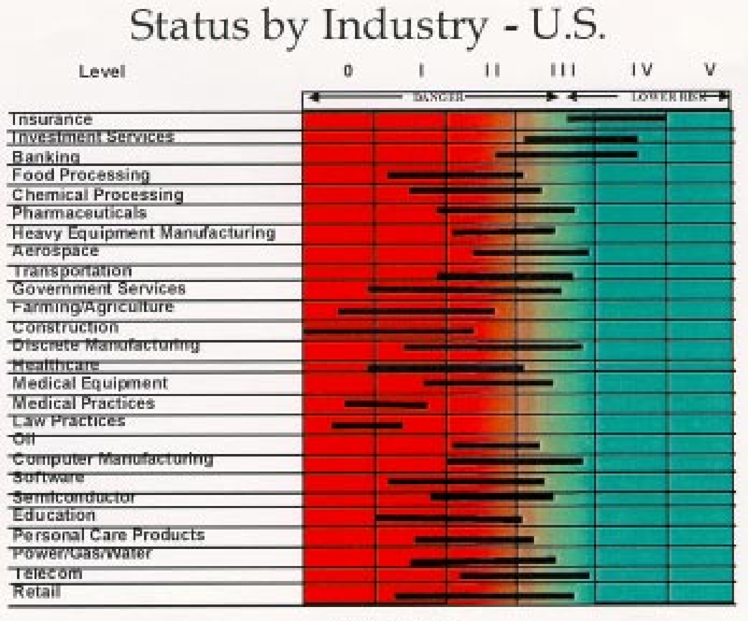
Insurance, investment services, and banking lead all other industries. Banking has a unique status, since small banks are lagging and large banks in the United States are ahead of many other industries. The insurance industry began having failures more than 10 years ago, and due to the critical impact their IT systems have on their business operations, they began their compliance efforts early. Banks in the U.S. began having failure problems nearly 30 years ago, but were not driven to begin compliance efforts until they were driven by regulation.

Infrastructure utilities and emergency services are critical for sustaining business operations and well-being. In the U.S., we predict that general infrastructure, power, non-wireless telephones, and critical services will continue mostly uninterrupted, with potential for relatively minor problems and some inconveniences. Natural gas utilities are lagging the utility industries. Healthcare lags in areas of medical practices, hospitals and elderly care. Public, private, and higher education also lag far behind. Many world governments are also far behind. The U.S. and Canadian governments are more than 40 percent ahead of any other government in the world, but lag large, private industry in the U.S. State governments differ widely in status. Most U.S. states have Year 2000 projects. 50 percent have reached the start of level III, and nearly all are being managed and driven from within IT. 65 percent of U.S. cities and towns do not have Year 2000 projects. Many mid-size and smaller cities and towns are lagging far behind or have not started. An industry highly overlooked is agriculture (farming, food processing, transportation/distribution, and import and export of foods and food bi-products). Several agriculture sub-industries are lagging far behind. Governments range from COMPARE level to level III, with the majority in level 0–II. (see Figure 3).


Status by Industry — Worldwide

Q 3 - September 1998

Figure 4 : *Status of Year 2000 Compliance - Industry View*

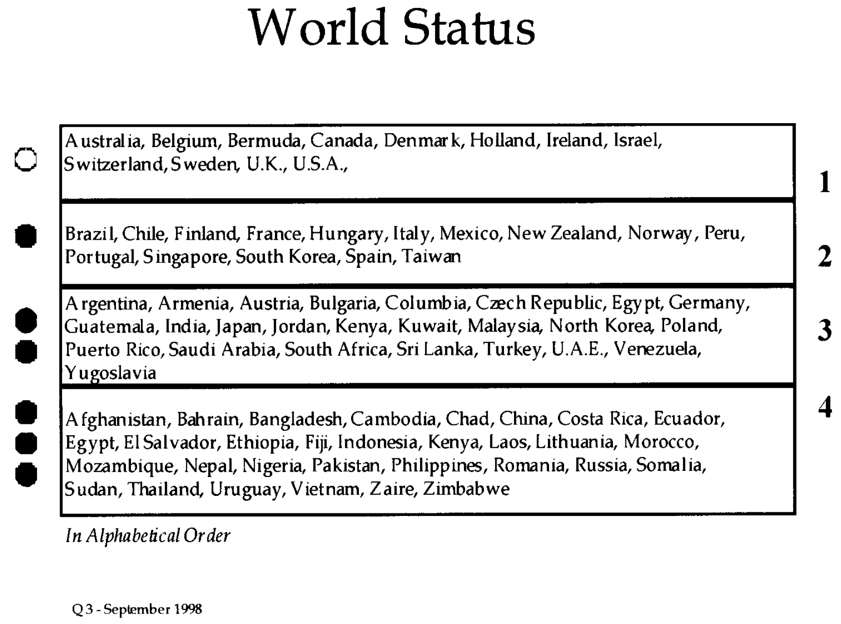

Status by Industry - U.S.

Q 3 - September 1998

Figure 5 : *Status of Year 2000 Compliance - U.S. Industry View*

CHARACTERISTICS BY COUNTRY

The largest impact this problem with have on the world is related to the global economy. Countries already plagued with financial woes, sharp increases in inflation, limited monetary reserves, and high unemployment are some of the same countries farthest behind with Year 2000 compliance. Figure 6 shows countries grouped according to level of risk and the predicted percentage of companies to experience failures. One white dot indicates that 15 percent of companies will have at least one mission critical system failure. One solid dot indicates that 33 percent of companies will experience such a failure. Two solid dots indicate that 50 percent will experience such a failure, and three solid dots indicate that 66 percent will experience the same. Infrastructure risks within a given country are shown separately in Figure 7. There are several key non-Year 2000 interdependencies considered when determining risks within a specific country, e.g., rate of inflation, shortage of food or key resources, current government out of favor with majority of people, risk of unrest, infrastructure failure risks, ability to import/export key goods or resources, likely dependencies on other countries for aid, and monetary reserves and world value of their currency. A number of countries already afflicted with several of these problems are considerably lagging in Year 2000 efforts, and will likely see even greater negative impact as a result.



World Status

○	Australia, Belgium, Bermuda, Canada, Denmark, Holland, Ireland, Israel, Switzerland, Sweden, U.K., U.S.A.,	1
●	Brazil, Chile, Finland, France, Hungary, Italy, Mexico, New Zealand, Norway, Peru, Portugal, Singapore, South Korea, Spain, Taiwan	2
●●	Argentina, Armenia, Austria, Bulgaria, Columbia, Czech Republic, Egypt, Germany, Guatemala, India, Japan, Jordan, Kenya, Kuwait, Malaysia, North Korea, Poland, Puerto Rico, Saudi Arabia, South Africa, Sri Lanka, Turkey, U.A.E., Venezuela, Yugoslavia	3
●●●	Afghanistan, Bahrain, Bangladesh, Cambodia, Chad, China, Costa Rica, Ecuador, Egypt, El Salvador, Ethiopia, Fiji, Indonesia, Kenya, Laos, Lithuania, Morocco, Mozambique, Nepal, Nigeria, Pakistan, Philippines, Romania, Russia, Somalia, Sudan, Thailand, Uruguay, Vietnam, Zaire, Zimbabwe	4

In Alphabetical Order

Q3 - September 1998

Figure 6 : *Research Countries and Failure Prediction*

In our country status and predicted failure rates within countries (Figure 6), the estimates include all companies and government agencies together. Venezuela started awareness efforts months ago, but a large number of companies and government agencies have not yet begun compliance efforts. The new government leader may affect the rate of progress. In Argentina, companies are finding it somewhat difficult to get funding for Year 2000 projects and consulting firms needed to supplement smaller companies are limited in number. Except for Israel, Middle Eastern countries are just beginning, and are lagging. In Russia, larger companies in just a few large cities are working on the problem, but companies throughout the country outside those cities are lagging far behind. Municipal services, healthcare, and other Russian industries are far behind. In Pakistan and India, only larger companies have begun efforts. In Mexico, the banking industry is aided by a regulatory process that succeeds in getting relatively accurate disclosures made. This helped to get the banking industry moving more quickly than other industries. Two years ago, companies in Japan did not believe they had a problem with Year 2000, but now many are trying address compliance.

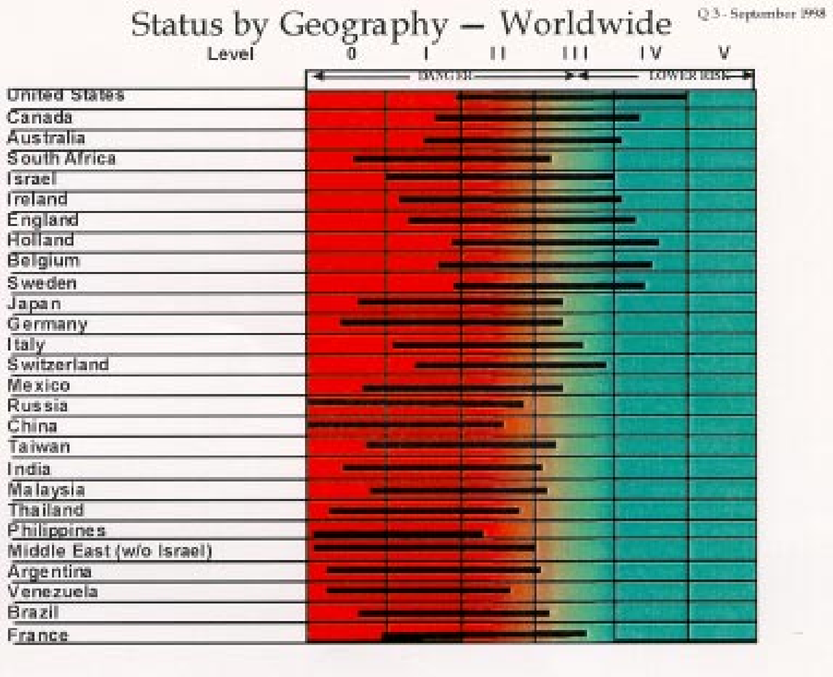
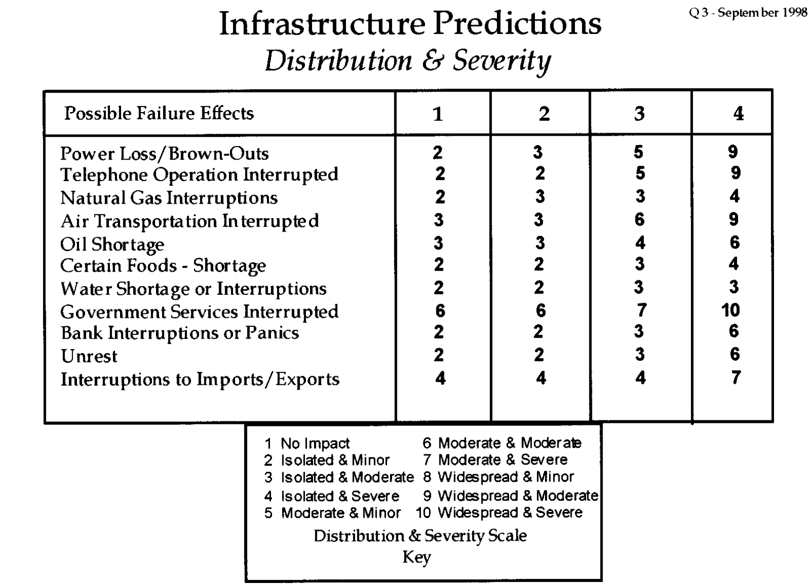


Figure 7 : *Sample of Countries Showing COMPARE Level*

The chart in Figure 8 shows the risk and probability of failure of basic infrastructure by countries. It shows a ranking of 1 through 10 that describes how widespread and severe infrastructure and service interruptions are likely to be for each group of countries (grouped in Figure 6). Each failure effect is ranked in each country category according to how widespread the impact will be realized, and the level of severity expected. The chart takes into account today's (as of Q3 1998) status and risks, interdependencies, levels expected to be reached by 2000, and likely failure results. Since some companies and governments will slow down or speed up their compliance efforts prior to 2000, and more and better status information is made available, this information will be updated periodically.



Infrastructure Predictions

Distribution & Severity

Q3 - September 1998

Possible Failure Effects	1	2	3	4
Power Loss/Brown-Outs	2	3	5	9
Telephone Operation Interrupted	2	2	5	9
Natural Gas Interruptions	2	3	3	4
Air Transportation Interrupted	3	3	6	9
Oil Shortage	3	3	4	6
Certain Foods - Shortage	2	2	3	4
Water Shortage or Interruptions	2	2	3	3
Government Services Interrupted	6	6	7	10
Bank Interruptions or Panics	2	2	3	6
Unrest	2	2	3	6
Interruptions to Imports/Exports	4	4	4	7

1 No Impact	6 Moderate & Moderate
2 Isolated & Minor	7 Moderate & Severe
3 Isolated & Moderate	8 Widespread & Minor
4 Isolated & Severe	9 Widespread & Moderate
5 Moderate & Minor	10 Widespread & Severe

Distribution & Severity Scale
Key

Figure 8 : *Distribution & Severity of Infrastructure Service Interruptions*
Note: countries included in the each of the four categories shown in Figure 8 are defined in Figure 6

FAILURE SCENARIOS AND PREDICTIONS

Each company and government agency is ranked according to its current status, its probability of gaining compliance, and the impact of technical systems on its typical business operations. After following failures and tracking status related to probabilities of failure, we show the relationship of status to predicted mission critical failure in Figure 9 (below). We now know that it takes approximately 30 months for a mid-size company to complete level IV and gain compliance of their mission critical dependencies.

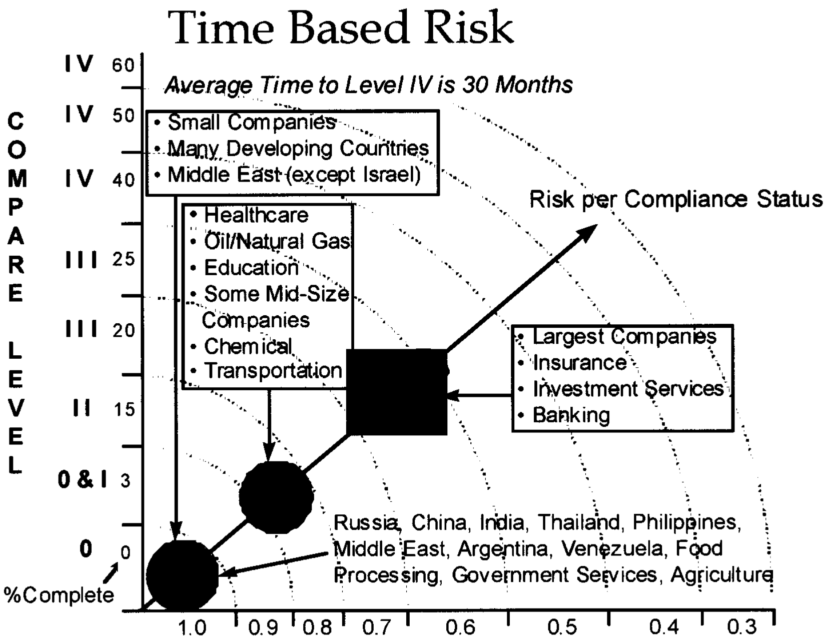


Figure 9 : *Risk versus Compliance Status - October 1998*

Using the chart in Figure 9, you can estimate high-level risk and probability of at least one mission critical system failure occurring within any company in an industry or government. This is done by using the current COMPARE status level and assuming it takes an average of 30 months for a midsize company to complete compliance of mission critical business dependencies.

PUBLIC PANIC AND SOCIAL ORDER

The economic and sociopolitical results from Year 2000 failures can include panic, unrest, increased crime, food and infrastructure interruptions, and health and safety issues. Social order may be affected when basic needs are disrupted. These affects are controlled by ensuring that basic needs will continue to be met and proactively reducing fear and disorder. Social disorder will be at risk in several countries and regions of the world, contributed to by Year 2000 failures.

CORE

To assess operational risk, to determine where contingency plans are necessary, and to develop contingency strategies, GartnerGroup uses a methodology called CORE (COMPARE Operational Risk Evaluation). It is used to determine risks related to supply chain, interdependencies, customers, investors, embedded systems, and IT systems. We recommend companies and agencies use CORE to determine operational risks and risks related to global dependencies.

CORE includes five steps or phases:

(1) Perform High Level Risk Assessment
(2) Inventory Business Dependencies
(3) Categorize Business Dependencies by Impact to the Business
(4) Perform Detailed Risk Assessment and Ranking
(5) Design and Implement Contingencies & Disaster Recovery

Use CORE to assess risks related to countries, infrastructures, industries, supply chain, or any business dependency.

ESTIMATED COST OF YEAR 2000

We estimate the total cost of Year 2000 to be:
—Worldwide IT Cost: *U.S. $300 billion to $600 billion*
—U.S. IT Cost: *U.S. $150 billion to $225 billion*
—*U.S. $1–2 trillion: Total worldwide cost*

WHEN FAILURES WILL OCCUR

System failures due to Year 2000 have been occurring for some time. They will increase in 1999, reach their highest volumes during 2000, and drop off during 2001. Few will continue past 2003. Contributing factors (all are 0.8 probability):

Software

(1) 83 percent of commercial software is not yet certified compliant—11 percent in April, 2002

(2) 4 percent of follow-on versions of commercial software will not be compliant

(3) 70 percent of custom solutions developed by a vendor more than seven years ago will not be supported by that vendor

Data

(1) 70 percent of archived data will not be remediated, but attempts will be made to use this data in remediated systems

(2) Non-compliant data will be passed to/from companies

(3) Some data centers will be shut down during rollover to reduce risk of failures

Systems

(1) Many IT systems will run non-compliant transactions during 1999, 2000, and 2001, since many are periodic transactions

(2) Some IT systems use applications that were frozen during 1999, but will be used again some time after 2000

EMBEDDED SYSTEMS

Embedded systems will have limited effect on Year 2000 problems, and we will see a minimal number of failures from these devices. Only 1 in 100,000 free-standing microcontroller chips are likely to fail due to Year 2000. A small percentage of real-time clock-driven chips are affected, but these failures will be a small percentage of the non-embedded system failures. The key issues concerning embedded chip failures are: (1) very few will fail, and (2) of those that fail, the majority will fail right at the millennium, and the majority of these will only fail once—if they are active when the clock ticks over. Embedded chips used for key infrastructure processes, life support systems, and other critical processes should be checked and verified by the manufacturer of the equipment, due to the potential severity and potential result of such a failure.

NUMBER OF COMPANIES & GOVERNMENT AGENCIES EXPECTED TO GAIN COMPLIANCE

In October, 1998, 15 percent of all companies claim to have achieved level IV compliance of mission critical systems. We predict that 50 percent will achieve this goal by 2000 (0.8 probability). The majority of large companies in Category 1 countries will complete at least 80 percent of level IV by 2000 (0.8 probability).

Predictions

- 1/1999 - 12/1999 - Fiscal year system failures begin to occur & testing begins
  11% of vendors default on compliancy of their products
- 7/1999 - 3/2000 - 30-50% experience a mission critical failure (15% in U.S.)
- 1/2000 - 1/2001 - 10% experience system failures within 12 months
  after Millennium
- 1/2000 - 12/2001 - 11% of commercial software continues to be non-compliant
- Exact impact on the world economy is not possible to predict, however Year 2000 will likely be one of numerous contributors to a negative impact over 3-5 years

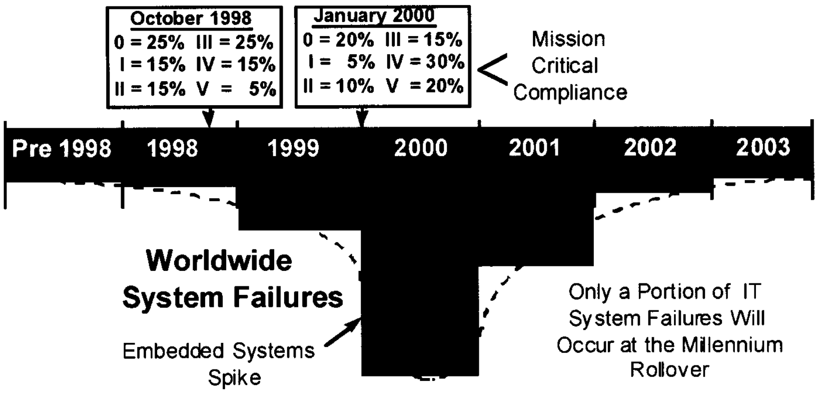


Figure 10 : *Predictions and When Failures Will Occur*

POSSIBLE RISKS TO THE UNITED STATES

Actions and proactive programs will be needed to keep these risks minimized, and keep them from materializing as described (see Recommendations).

Domestic

(1) Interruptions due to failures in interdependencies and interconnections between companies and countries produce significant negative impact for U.S. businesses and government operations
(2) IT systems in critical industries will not be fixed in time
(3) Global impact from Year 2000 is not adequately planned for and Year 2000 fuels global recession much more than anticipated
(4) U.S. foreign investments encounter disastrous results and significantly impact the U.S. investment market
(5) Too many people lose confidence in the banking sector
(6) Too many interruptions occur in food or medical supply chain
(7) Local city and town governments cannot provide critical services
(8) Foreign loans, pacts, and trade agreements are adversely affected

Foreign

(1) Public panic or loss of confidence in the banking sector in high risk countries
(2) Global economy impacted by foreign business and government interruptions
(3) Foreign loans, pacts, and trade agreements are adversely affected
(4) Aid or bail-outs are needed for highest-risk countries
(5) Foreign business interruptions impact too many U.S. companies
(6) Foreign security issues ignited by unrest or severe economic issues
(7) Key foreign government agencies experience significant failures

RECOMMENDED ACTIONS FOR THE U.S. SENATE

(1) The United States has no body or group tasked with full time monitoring and analysis of global risks the Year 2000 problem is likely to pose to the United States.

Even if advisory or consulting companies were to provide this information to the U.S. Senate or other bodies, a full time effort is needed to coordinate global risk assessments of U.S. and foreign governments and other risk threats from other countries on a regular basis—and, even more importantly, to take subsequent emergency action and launch pre-failure contingency plans to reduce risk and ward off possible serious effects. There also needs to be a focal point for providing risk information and warnings to the American public.

Recommendation: Identify one current federal agency (as a Global Risk Management Agency) to manage and coordinate global impact of the year 2000 problem on the United States. Economic, financial, monetary, military, political, and other resources will need to be analyzed regularly, and quickly-developed strategies and contingencies will need to be launched across agencies, political governing bodies and foreign governments. This agency should report to the Executive Office, and have immediate access to the President's Cabinet in matters of foreign policy, aid, funding, and national security. It should provide press releases, information, guidelines, and warnings to the American public with regard to industries, infrastructure, government, and personal risks throughout 2001.

(2) Many Federal programs are administered locally, and many local governments lag in Year 2000 readiness. Therefore, interfaces between levels of government are at risk. These include interfaces and transactions that occur between local, state, and Federal Government Agencies. Local cities and towns are lagging far behind and need expertise, information, awareness, and aid, to combat the Year 2000 problem.

Recommendation: Launch U.S.-wide program to coordinate efforts with State and local governments and provide special local city and town government aid and information. This effort should be guided by the Global Risk Management Agency (described in number 1 (above).

(3) Our experiences shows that U.S. companies are not providing accurate disclosures related to Year 2000 risks and contingencies. There are considerable differences between the status of Year 2000 compliance and critical risks that companies disclose to the SEC, and what the actual status and risks are within that company. This increases the risk of public investments being made without full understanding of Year 2000 risks.

Recommendation: Pass legislation or require the U.S. SEC to implement random audits as part of the Year 2000 disclosure and reporting requirements for publicly held companies in the U.S. We suggest a sample of audits be conducted by an outside audit agency to confirm these findings, and then change the SEC policy to include sample audits as part of the routine process of Year 2000 disclosure, if substantiated with the sample audits.

(4) U.S. Senate and U.S. federal government Year 2000 plans and contingency plans seem to assume that most failures will occur when we hit January 1st, 2000. As described in this testimony, failures will occur heavily from 1999 through 2001, and not over one single day or week.

Recommendation: Set correct expectations in U.S. government agencies, with U.S. government contingency plans, and with foreign governments that the failure window will be a three-plus-year period. Ensure that the SEC disclosure period and other Year 2000 regulatory government efforts are planned to last during the entire period needed.

(5) Many lagging companies and government agencies in the U.S. are being asked to implement new regulations, rules, reports, and processes in their IT systems and data to support new federal requirements or legislation continually being passed by Congress (pertaining to a specific industry or segment, e.g. healthcare, education, telecommunications, etc.). This is a major contributor to lack of progress in these companies. Most best-in-class companies farthest ahead in gaining compliance have frozen or significantly reduced enhancements to current IT systems. This has allowed them to focus on fixing the systems and other business dependencies.

Recommendation: Question all new legislation to determine if it may require IT modifications (i.e., software, hardware, data, or automated reports) in federal, state, or local government agencies, or in private companies. Cease and desist from passing or enacting any legislation that may affect IT systems or change reporting data. Such bills should be put on hold for an extended period, to allow companies and agencies to be successful in their compliance efforts. This will reduce the risk of non-completion of compliance for healthcare, education, and federal, state, and local government by 30–50 percent.

(6) The U.S. Government efforts appear to be focused in two areas: (1) IT systems within federal agencies and (2) launching legislation to help support compliance within critical industries. It is now clearly evident that segments of companies and governments throughout the world will not be fully prepared to deal with this prob-

lem by 2000. Significant global impact will be realized without immediate action to avoid moderate or worst case results.

Recommendation: We suggest adding a 3rd area of effort—managing global dependencies and risks. It's critical to launch substantial contingency efforts in order to reduce global dependency risks prior to Q3 1999. These efforts may be conducted by the Global Risk Management Agency (described above). We suggest this new and additional focus be defined as a major component of U.S. national compliance efforts, and directly linked to the U.S. federal agency efforts, the Executive Office of the federal government, and the U.S. Special Committee on Year 2000.

SUMMARY

A great deal of progress has been made during the past year in the U.S. and in several parts of world. IT organizations in the U.S. have increased their spending for Year 2000 projects an average of 6 times over what was spent during 1997. Year 2000 is now prioritized at the top, or number 2 (following Enterprise Resource Planning system projects—to replace Legacy systems) by most U.S. companies. Large companies in the United States have made the most significant progress, and many of them will complete most of their compliance efforts by 2000. Even smaller companies in the United States have made significant progress in the past year, in several industries.

Even with all of this progress, there are still very serious risks for the United States and throughout the world. The gap is widening even more, between companies and governments farthest ahead and the ones farthest behind, since the laggards are moving much more slowly toward compliance. In the United States, industry segments such as healthcare, education, agriculture, construction, food processing, governments, and companies under 500 employees are lagging way behind in compliance efforts. Many of these will simply not finish critical systems by 2000.

U.S. investors are provided very optimistic , often inaccurate, disclosures from publicly traded companies (to the U.S. SEC), and therefore accurate investment risk assessment data is not often available. This is likely to affect our U.S. market and several other economic factors as we get closer to 2000.

Interdependencies and interconnectivity between companies and across country borders are also extremely high in significance related to Year 2000 risks. Many of these interdependencies are not being covered by either company, and many times these interconnections and data transfers cannot be easily tested. These are of critical importance in banking, government, healthcare, and for many global manufacturers.

Even if we were to miraculously fix every one of these domestic issues and make certain all U.S. companies and government agencies will get themselves Year 2000 compliant before 2000, the absolute largest risk to the United States and to U.S. citizens is the impact from companies and governments outside the United States. Far too many companies and governments critical to our continued strong economy, and providers of key resources, are more than 30 months behind private industry in the U.S. Since it takes an average of 30 months for a midsize company to achieve compliance of their most critical systems, many of these lagging foreign companies and governments will simply not have enough time to get their systems fixed before 2000. Failures will lead to a negative impact on our economy and availability of critical resources. We'll see significant impact from failures in these regions, including economic, sociopolitical, investment shifts, market changes, critical resources, national security, and defaults on federal loans. The only way now to combat this enormous issue, is for the U.S. Government to launch significant foreign contingency strategies in order to reduce or negate high risk dependencies on these industries and countries before we begin to feel these ill-effects. Since failures will increase in numbers throughout 1999, increase in volume throughout 2000, and continue at reduced levels throughout 2001, the time to act on this is now.

PREPARED STATEMENT OF SENATOR DANIEL PATRICK MOYNIHAN

As we wind up the last Year 2000 (Y2K) hearing of this Congress, I would like to commend Senator Bennett and the Special Committee for its work in addressing the computer problem. The Committee has done a fine job in looking at all the aspects of society that the Y2K problem affects: the utilities industry, the heath sector, financial services, transportation, government, and businesses. The Committee should also be applauded for the role it played in formulating and passing S. 2392, The Year 2000 Information and Readiness Disclosure Act. As an original cosponsor of this piece of legislation, I am pleased to see that its enactment is soon at hand. The head of the President's Council on Y2K, John Koskinen, said that passing this bill is one of the most important things that we could do on the Y2K front. I agree. I say well done to the Committee for all of the work it has done in such a short amount of time.

It was almost two and a half years ago that I sounded the alarm on the computer problem. On July 31, 1996, I sent President Clinton a letter expressing my views and concerns about Y2K. I warned him of the "extreme negative economic consequences of the Y2K Time Bomb," and suggested that "a presidential aide be appointed to take responsibility for assuring that all Federal Agencies, including the military, be Y2K compliant by January 1, 1999 [leaving a year for 'testing'] and that all commercial and industrial firms doing business with the Federal government must also be compliant by that date."

January 1, 1999 is quickly approaching. I believe that we have made progress in addressing the computer problem and that the "Good Samaritan" legislation will play a significant role in ameliorating this problem. But much work remains to be done. For the next 450 days we must continue to work on this problem with dedication and resolve.

Historically, the fin de siecle has caused quite a stir. Until now, however, there has been little factual basis on which doomsayers and apocalyptic fear mongers could spread their gospel. After studying the potential impact of Y2K on the telecommunications industry, health care, economy, and other vital sectors of our lives, I would like to warn that we have cause for fear. For the failure to address the millennium bug could be catastrophic.

PREPARED STATEMENT OF DR. CHARLES POPPER

Good morning Mr. Chairman and members of the Committee. My name is Charles Popper and I am Vice President of Corporate Computer Resources at Merck & Co., Inc. In that position, I serve as the chief information officer of Merck.

Thank you for inviting me to participate in today's hearing on the Year 2000 problem. I applaud this Committee's efforts in both investigating and publicizing the potential effects of this very serious and prevalent computer bug. I would like to discuss what my company, Merck, is doing to deal with the problem. I would also like to provide a broader context that you may find useful.

Merck is a global research-driven pharmaceutical company that discovers, develops, manufactures and markets a broad range of medicines, directly and through its joint ventures, and provides pharmaceutical benefit services through Merck-Medco Managed Care. Merck remains the oldest and largest U.S.-based company dedicated to innovative vaccine research, development and manufacturing. Merck believes in focusing its efforts on the discovery of important new medicines. The Company will spend almost $1.9 billion on research and development in 1998. Merck's pharmaceutical manufacturing operations encompass 30 plants worldwide in the United States, Europe, Central and South America, the Far East and the Pacific Rim.

Y2K AND MERCK

As you know, the Y2K bug can potentially affect any computer program that processes dates, including software application programs, operating system programs, and firmware programs that are embedded in countless devices that are relied upon by companies and consumers alike. Our task at Merck has been to ensure that all such programs that are in use anywhere within Merck's world wide operations will operate correctly throughout the transition to the new millennium.

But our objective all along has been a more important one, consistent with Merck's company mission. As George W. Merck stated many years ago, "we try never to forget that medicine is for people." Merck is solving its Y2K problem is order to ensure that we can continue to discover, develop, manufacture, and distribute medicines that treat important human diseases. Our paramount goal is to ensure the continuity of the supply of medicines to our patients.

MERCK'S Y2K PLAN

We are doing so by following a simple strategy.

—First, we have inventoried all computer systems, applications, and devices with embedded processors.

—Second, we have assessed each of these systems to determine whether it includes any date processing and whether its correct operation is of serious concern to our business. As an example of a system where we are less concerned about a possible Y2K bug, consider a program that reports monthly sales and organizes the columns of the report in chronological order. While we prefer to have the report continue to show the most recent results from right to left, if the Y2K bug were to merely cause the columns to print in a different order, this would be only a minor concern. We are deferring the repair of such bugs to the final stages of our Y2K project.

—Third, we have developed a compliance strategy for each system. That is, we have decided whether to repair the software, to replace it with a newer version that is Y2K compliant, to retire the system from active service, or to simply let it fail (as in the above sales report example).

—Fourth, we are executing the strategy for the many thousands of systems in our inventory. This is obviously a daunting task, because of its magnitude and its geographic diversity; we have to deal with systems in the many hundreds of Merck locations world wide. Hence we have put in place an elaborate management tracking and control system, to ensure that nothing falls through the cracks.

—The fifth and final step is to thoroughly test all of our systems. Our attitude is to trust no one but ourselves. If a system vendor tells us that their application is Y2K compliant, we will insist on testing it ourselves or at least auditing in detail the test results provided by the vendor. We have already found instances of applications certified compliant by the vendor that, in fact, did not pass our tests initially.

Our goal has been to achieve Y2K compliance by the end of this year, thus allowing all of 1999 for dealing with the inevitable glitches and inconsistencies among systems. We have also planned from the outset to use 1999 for the global deployments of remediated systems. Many of our systems and applications are deployed in multiple manufacturing plants, headquarters sites, and research laboratories. It is really not necessary to deploy the corrected system everywhere this year; it suffices to successfully test one instance of the system, so that we can safely plan additional deployments next year. The actual deployment schedule is designed to minimally disrupt our ongoing operations.

As you can imagine, Merck's Y2K Project is a very significant effort. We began reasonably early, in 1996. There are now in excess of several hundred people involved; we are spending many tens of millions of dollars to plan, execute, and manage this work. By starting early, we were able to schedule the resources in such a way as to have less impact on both ongoing business operations and the other information technology initiatives so important to Merck's continued success.

MERCK'S BUSINESS PARTNERS AND Y2K

Fixing our internal systems is only part of the problem. Merck, just as any global company, works with many thousands of business partners, suppliers, customers, and government agencies. Our ability to continue our company's operations successfully in January of the year 2000 depends just as much on the Y2K programs of these companies and agencies as on our own internal systems. Hence we have organized two other major sets of activity:

—Each business area is examining its business partners to assess its Y2K risk. If the proper operation of that entity's systems is essential for Merck's operations, we are both working with that entity to better understand its Y2K remediation plans and also developing internal contingency plans just in case that entity fails to achieve Y2K compliance on time.

—We are also working as part of the VitalSigns 2000 Project, an effort sponsored by the Odin Group, to gather important information about the Y2K compliance of the entire health care industry in which we participate. This is the only systematic effort of its kind, whose objective is to map out the cross-industry processes that together provide American patients with health care services. The VitalSigns 2000 team has developed a survey instrument for the five groups of entities comprising the health care industry: payers, providers, suppliers, distributors, and government agencies. The survey is collecting information about the Y2K readiness of each of these sectors, as well as their interdependencies. By understanding the cross-industry processes and their Y2K vulnerabilities, we, together with the rest of the industry, can develop the detailed contingency plans that can assure the continuity of high quality patient care.

Y2K AND THE PHARMACEUTICAL INDUSTRY

What about the broader American pharmaceutical industry? While I obviously cannot testify about the detailed plans and projects of Merck's competitors, I have had the opportunity to discuss the Y2K problem with my colleagues in other pharmaceutical companies, as we've worked together within PhRMA, the Pharmaceutical Research and Manufacturers of America. These companies have all followed a methodology similar to Merck's and are applying the level of resources needed to deal with the problem. They have also recognized the broader issue of the readiness of business partners and are developing appropriate contingency plans.

We hope that our colleagues and counterparts elsewhere in industry and government are diligent in their efforts, so that America's health care system is unaffected by Y2K.

CONCLUSION

Let me close with some broader context. I read periodically about companies and agencies that are just now waking up to the severity of the problem. Worse, I still read and hear about entities that still do not believe that there is a serious problem. They may be right, in their local situation, but only an organized testing program will allow them to be sure. So I do worry about what will happen as the clock strikes midnight December 31, 1999.

The key to success will be our overall preparedness. Hence the work of this Committee is of vital importance. It is essential that you keep the pressure on both industry and government, both to minimize the number of system failures we experience and to maximize our readiness to deal with the problems that do occur.

Again, I thank the Committee for the opportunity to be here today and look forward to your questions.

Responses of Dr. Charles Popper to Questions Submitted by Chairman Bennett

Question 1. Mr. Popper, Merck & Co. is as international in its operations as an American company can get. You have heard Mr. Marcoccio's comments on the severity of the international Y2K problem. From your perspective as the CIO of an international company, what more do you think the United States should be doing to head off this developing storm cloud?

Answer. I believe that the U.S. should focus on two key areas. First, we must provide strong leadership on the Y2K issue by setting an example for other countries. All segments of the federal government must do whatever it takes to prepare for the Millennium Bug—there must be adequate plans as well as determined management and follow up. We need to demonstrate to other governments both the seriousness of the problem and the techniques and resource commitment needed to address it properly. Second, we should work to enable adequate international disclosures of Y2K readiness. We can do this by encouraging other countries to emulate the recently enacted Year 2000 Information and Readiness Disclosure Act [S. 2392], and by working through the appropriate international organizations to enact similar international protection.

Question 2. Laurene West testified about her personal medication Y2K problems, which provides a unique perspective. How do you see the pharmaceutical supply chain responding to that kind of short shelf-life medication issue?

Answer. I believe that the supply of short shelf-life medications to patients can best be assured by allowing each pharmaceutical company to address its own specific problems. Each company knows its products, its customers, and its supply chain alternatives best. Each company can therefore develop the contingency plan that best meets its unique situation and the needs of its customers, including the issue of short shelf-life medications. Any broader action—especially one that attempts to implement a common contingency plan—would only add risk, by putting all of our eggs into one basket.

Question 3. Recently, the CIO of another major pharmaceutical company told our committee that in the next 3–6 months they will begin a "flight to excellence" which means the company will begin cutting off suppliers or business partners who cannot demonstrate that they Y2K ready. Is Merck considering any similar actions? Would you consider this "flight to excellence" a good way to promote Y2K readiness on a business to business level?

Answer. Merck is certainly examining all of our suppliers and business partners, and, if we are not satisfied with their plans for Y2K readiness, then we are formulating contingency plans. One element of the plan might include seeking alternate sources for those goods or services. An alternative is assuring the availability of supply through the expected duration of supply chain interruption. The key is to develop and implement an effective contingency plan for each critical product or service, drawing upon our knowledge of the state of readiness of our suppliers and partners. In this way, we can ensure that we continue to meet our customers' needs.

Question 4. Mr. Popper, the pharmaceutical products your company produces are dependent on suppliers for ingredients and distributors for sales to the ultimate consumer. Where do you see the most critical interconnectivity points?

Answer. Our analysis of the Y2K risks created by our suppliers and customers is an ongoing effort, which we expect to continue throughout the balance of 1998 and all of 1999. So it is inappropriate to identify the most critical risks on a "once and for all" basis. Right now, our assessment is that the most important risks are within the power utility, transportation, and government sectors.

Question 5. Mr. Popper you mentioned the VitalSigns 2000 Project that Merck is participating in as a contributor. How do you see this helping to bridge the Y2K problems in the Health Care industry?

Answer. The Vital Signs 2000 Project, sponsored by the Odin Group, is intended to identify the major Y2K risks of the entire pharmaceutical supply chain, including suppliers, distributors, providers, and payers. The survey will identify those industry segments (or their suppliers) who are less likely to be prepared, so that we can prioritize and prepare good quality contingency plans. We are also working to develop templates for contingency planning that will be made available to the entire industry. We expect two benefits from this effort. First, it will enable even small companies to prepare good quality contingency plans. Second, it will allow all companies to more easily examine the readiness of their business partners in a standard way; this too will facilitate better and more consistent contingency plans.

Question 6. Mr. Popper, we've heard a lot today about small and medium sized businesses. We heard from another witness that these firms tend to "not" pay attention to the Government and it's communications. However, they do listen to their trade associations. Do you think enough is being done to inform the small and medium sized players in the pharmaceutical sector? What more can be done, say with trade associations?

Answer. I believe that a reasonable answer to the issue of small and medium sized players will emerge from the Vital Signs 2000 survey; prior to analyzing the survey results, I cannot assess how ready these industry segments will be. Using trade associations to inform and support smaller companies is probably a good idea. Here, too, it might be feasible to leverage the template and contingency planning expertise developed by the Vital Signs 2000 project.

Question 7. Mr. Popper, could you please describe to the Committee the kind of contingency planning that is required for a firm of your size to cope with the Year 2000 problem?

Answer. In brief, our challenge is to be prepared for all reasonable contingencies. We have identified all of our suppliers of both goods and services, and we have assessed the risk and impact of supply interruptions for each supplier. We then prioritized the suppliers based upon this risk/impact assessment. Finally, we are working through this prioritized list to prepare reasonable contingency plans. In addition, we intend to form emergency response teams to deal with the unexpected problems that will inevitably arise when we roll over into the new millennium.

One caveat is in order. There are contingencies that are impractical for even Merck to prepare for. For example, it is conceivable that scattered electric power outages could spread via the power grid to black out major portions of the country. We cannot prepare to overcome such a circumstance. This is, in fact, where we rely upon the U.S. government to help. If it were concluded that scattered power outages are likely or even possible, we would hope that there would be planning at the federal level to prevent these from spreading. As our own planning proceeds, we would be happy to share with the Committee any findings of similar contingencies that we believe would benefit from federal attention.

Prepared Statement of Rod Rodrigue

It is an honor to be before this Committee to bring to you information with regards to the Year 2000 problem. All of you have been inundated with studies which attest to the negative economic impact on this country's 384,000 manufacturers.

A national study indicated that 7 percent of small manufacturers could shut down and an even greater number would experience varying degrees of business interruptions. The national negative impact exceeds $150 billion. It is our estimate that if these figures hold true, Maine would experience a negative impact in excess of a quarter of a billion dollars.

I am here today with good news that there's a national system armed with an effective tool to positively impact the Y2K problem. Several months ago the Department of Commerce's NIST/MEP program developed an assessment tool, which allows MEP engineers to quickly, and accurately organize the broad spectrum of Y2K issues faced by today's small and medium-size manufacturers. The use of this project management tool gives the small manufactures a road map for addressing the most critical issues such as accounting systems, computerized production equipment, environmental management systems, as well as external threats.

The most exciting aspect of this tool is that it now resides in the hands of 2,500 men and women located in 400 offices in 50 states and that its implementation can be coordinated under a single unified national effort at MEP headquarters. The MEP centers are linked to over 3,500 partner agencies, which can be called upon to help disseminate the Conversion 2000 tool. I believe that for the first time we can present to you a viable mechanism for attacking the millennium problem.

Under the leadership of Senators Snowe and Collins Maine has progressed beyond the design stage and proceeded directly into implementation in over 100 companies. Utilizing a call center in contacting 2,500 Maine manufacturers, we confirmed what many studies have concluded. Despite having knowledge of the Year 2000 problem over half of the small manufactures had no plan to take any action before the turn of the century, and those who wanted to act were having great difficulty in organizing a systematic approach to the problem. After recognizing that between 500 to 600 small Maine manufacturers would need immediate assistance, the Maine MEP built a broad-based coalition which included Chambers of Commerce, Economic Development Districts, Small Business Development Centers, volunteers and business visitation specialists. These agencies, as well as independent consultants, will be trained by MEP engineers to deliver the Y2K assessment tool throughout the Maine manufacturing community.

Technical experts will staff Y2K hot lines on a 24-hours basis. Once the assessment has been completed MEP engineers will generate a report which clearly defines the necessary remedial steps. Accompanied with this report will be a single-page instruction sheet on how to apply for a Small Business Administration (SBA) LowDoc/Fastrack loan. The finalized report will not only facilitate loan processing but will also provide a standardized industry accepted document which will demonstrate the manufacturers due diligence in becoming compliant for their banks and other trading partners.

As president of the Maine MEP I have been asked what the committee can do to assist small manufacturers at this crucial juncture. On behalf of the millions of men and women who work in small and medium-size manufacturing facilities, I respectfully request the committee to appropriate the necessary funding to allow the MEP system to implement the Y2K tool at the national level. It is important to understand that this is an assessment tool and that we must complete this work on an expedited basis in order to allow these manufacturers to complete the identified problems in time.

ADDENDUM TO ROD RODRIGUE'S TESTIMONY

Along with the testimony submitted at the Y2K hearing, I believe that it is incumbent upon me to mention the importance of appropriating additional funding to help the Manufacturing Extension Partnership's (MEP) initiative in developing a national Y2K program like Maine MEP's. The MEP is committed to helping U.S. manufacturers in addressing the Y2K issues. To implement the Y2K program additional resources would assist states like New Jersey. Robert Loderstedt, President of New Jersey MEP, has indicated to me that of the 13,000 small manufacturers, New Jersey faces a potential closure of 1,000 businesses in Year 2000 and between 2,000–3,000 others needing assistance in becoming Y2K compliant. Although Maine needs additional appropriation to address the Y2K problems, New Jersey, as well as other states, clearly has a great financial need in tackling their manufacturers' Y2K issues.

RESPONSES OF ROD RODRIGUE TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question. In your testimony regarding the NIST/MEP Conversion 2000 assessment tool, you indicated that within Maine you have progressed beyond the design stage with over 100 companies engaged using the tool and MEP assistance. When did these efforts start? How long does it take to complete an assessment with Conversion 2000 and MEP representatives? What can you tell the committee about the results of those efforts to date? Are there any lessons learned to share at this point?

Answer. The efforts started in early September as soon as we had first results from our call center that was set up to directly, individually, and personally raise manufacturer awareness of the Y2K problem.

Complete assessments with Conversion 2000 and a MEP representative are determined by the size of the company and scale of their specific problem. We have some companies that are relatively small and without significant computing resources that feel they don't need any help at all. We can educate them that Y2K is not just an internal computer problem but a more generic business problem with both internal and external considerations. These companies, once aware of all the potential exposures, can be helped fairly quickly (one or two visits and letters between suppliers) because of their limited exposure. For other companies it has taken our very pointed calling awareness program to bring focus to the Y2K process (quite late I think) and they are in much more significant jeopardy, taking longer to complete. A case in point is one company that sources all it's raw materials from five different European countries with five currencies, has a third party broker to clear customs for these products, and being a catalog company depends on another third party mailing list provider for its market. This company also has manufacturing operations that may have an embedded chip concern. Considering that Europe is significantly behind the United States in its Y2K efforts and that the Euro common currency will be rolled out at the same time as Y2K hits, this company has a much more complex situation than others and will take longer to assess. This is only one case but there are many more that once a MEP representative has called and explained the whole realm of possibilities are finding that this is in fact a real problem for them that they are having to deal with and are not prepared.

To date we have identified through our call center 250 Maine companies that have indicated they would like to have a field engineer call. We have assigned MEP representatives to 206 of these companies and are currently working directly with 30.

There is a lot of apathy in the marketplace and it takes a concerted effort to get businesses to recognize their exposure. This is more of a problem for companies than they originally recognized and they have to devote more time to it than ever envisioned. MEP needs to be involved in the assessment phase because without some concerted effort many of these companies will not come to the process until it's too late. MEP needs to provide funding for the assessment phase of Y2K because it's a good investment in our business future. A small expense now in assessment can mitigate far larger costs later.

Question. You have asked the committee to appropriate the necessary funding to allow the MEP system to implement the Conversion 2000, Y2K tool, at the national level. What is the necessary funding needed at the national level? How would you propose that the funds be administered to discourage abuse and encourage proactive Y2K efforts? If federal funds were made available for a national MEP effort, how would you propose those non-manufacturing businesses are given similar assistance? Is it appropriate for the Federal Government to accept these costs and where should it stop?

Answer. Based upon our estimates for the needs of Maine manufacturers, we believe the funding needed at the national level is at least $50 million for expanding the Y2K outreach initiatives of the MEP system. These funds would be best managed through the national MEP program, as the federal funds added to the cooperative agreements of the manufacturing extension centers would leverage the match funding requirements from the states and local partners. This means that if the Federal Government provides half of the needed total, the match funding requirements would effectively bring $50 million in resources to bear upon this critical need.

An expanded MEP outreach effort would benefit non-manufacturing businesses through expanded partnerships with Export Assistance Centers and Minority Business Development Centers within the Department of Commerce, Small Business Development Centers (SBDC's) of the SBA, and Department of Agriculture extension offices. We have been working with the SBDC's of Maine to help streamline the loan approval process for SBA Y2K remediation project loan guarantees. The Utah and Iowa MEP centers have partnered with SBDC's to provide Y2K awareness materials and presentations. The Department of Commerce recently signed an MOU with the Department of Agriculture under which MEP is providing Y2K awareness materials, Y2K Self-Help Tool, and training. Discussions are continuing with the Department of Agriculture and SBA for replicating these successful partnering models across the national system, if additional funds become available.

The MEP Y2K outreach program takes a company through the awareness phase and helps a company determine which of its systems are not Y2K compliant. It then helps a company plan the necessary remediation and identify the resources required to implement the corrective actions (such as SBA loan guarantees). At that point it is the company's decision to commit its own resources to proceed with the remediation project. Federal funds will not be used to repair systems for companies, but we believe that it is appropriate for the Federal Government to expand its Y2K outreach efforts in continuing awareness and assessment activities to help small businesses identify the extent of their Y2K problems.

Question. As a result of the Conversion 2000 assessment process is a report defining necessary remedial steps generated by MEP engineers, according to your testimony. You note the report will both facilitate SBA loan processing and demonstrate due diligence. Has the SBA agreed to accept this report as the basis for expediting loans? How do small manufacturing companies using Conversion 2000 generate this report? Will the SBA accept a report not generated by a non-MEP engineer?

Answer. For matters of SBA policy please contact Kris Swedin, SBA Associate Administrator for Legislative and Congressional Affairs. Kris may be contacted at SBA headquarters at 202–205–6700.

Maine MMEP, Maine SBA and the Maine SBDC have developed a partnership where the MMEP Assessment will be utilized by the SBDC to put together the financials and business plan for any company needing capital to meet it's Y2K needs. The SBA will work with the SBDC and it's lending partners to ensure that no business lacks the capital for Y2K conversion. We believe that this model could be used in other states.

Question. The need to continue awareness campaigns at this late date continues to trouble this committee. However, it is been more troubling that once made aware of Y2K issues, over half of small and medium size manufacturers in Maine plan to take "No Action." Would you please describe your sensing of why this course of action ("No action") is selected over 50 percent of the time? What is being done to educate them as to the consequences of taking "no action"?

Answer. We believe that the reason for many companies deciding not to act is the lack of a complete understanding of the pervasiveness of the Y2K problem and how it can effect their business. Many companies are "generally aware" of the problem, but have not taken the time to investigate the potential effects of failures within external organizations upon which they rely, within their own embedded systems, or in their "relatively new" systems which they assume are compliant. A more proactive and detailed awareness campaign is needed to target this large group of small businesses to break through these misperceptions and apparent apathy about the Y2K problem. A portion of funds made available for expanding the national MEP Y2K outreach effort would be used for a more in-depth awareness campaign for small businesses.

PREPARED STATEMENT OF HAROLD SCHILD

Chairman Bennett and committee members, I thank you for providing me an opportunity to share with you our experience as a relatively small, farmer owned, dairy cooperative, in dealing with the year 2000 computer problem. I'll provide you with the full text of my comments but only recap the highlights in my remarks here before you today.

FIRST NOTICE

We were first made aware of possible Year 2000 problem during February 1996 audit of our 1995 financial records by a big five auditing firm.

At the management level, we authorized our Management Information Services staff to research the validity of the potential for problems in our computer systems. They reported that there was indeed a real danger of a complete calamity when January 1, 2000 rolled around and we should begin immediately to work toward correcting the problem.

MAGNITUDE OF THE PROBLEM

TCCA is a 150 member dairy cooperative nestled between the Coast Range Mountains and the Pacific Ocean 75 miles west of the Portland, Oregon metro area. The association has sales of about $160 million, totally in branded, value-added dairy products, primarily cheddar cheese, a small sample of which I've shared with you today.

At the time we became aware of the Y2K problem we had an M.I.S. staff of two people. Despite our efforts, we have been unable to attract additional staff to our coastal area to cope with every day programming demands, plus deal with the Y2K bug. Many other companies, IN THE METRO AREA, able to pay higher salaries, have engaged most of the qualified PROGRAMMERS in the region.

Our approach was to form teams that would think of all the potential problems in their areas. Some of our people were sent to seminars to gain a better understanding of where to search for the Y2K bugs. A few of the potential problem areas they found were:

1. Accounting software
2. Electronic Data Transfer (E.D.I.) between TCCA and customers
3. Member and employee payroll
4. Point of sale programs (Visitor's Center/Farm Store)
5. Were our suppliers compliant
6. Legal issues—performance agreements
7. Financial transactions—customer payments
8. Order reception and processing—customers complaint?
9. Automated product processing—would the plant produce product?

To date, our accounting department estimates that our out of pocket, cash expenditures will exceed $1 million to avoid a major Y2K problem. This does not include any of the internal cost of staff time or expense for training. The loss of productivity internally, because our people were busy with Y2K, is also not included in this cost estimate. This cost will be directly borne by our dairy members many of whom are struggling to make ends meet already.

CURRENT STATUS

At the present time, we are applying a test program to all of our software to determine if all bugs have been exterminated. We are confident that TCCA will be Y2K ready before the fall of 1999 if we do not experience delays in receiving software, which we have contracted for installation April 1, 1999. We expect no problems, but then I'm sure there will be some surprises, there always are.

FOOD INDUSTRY'S READINESS

Many CEO's of dairy companies I talk to express a wide range of views on Y2K from disbelief that it is more than a computer industry hype to stimulate business, to a view that the electronic world as we know it will cease to operate, leaving commerce stalled, utilities shut down, and only hand operated equipment functioning. Some project no additional cost to complying with Y2K requirements while others estimate their costs will, like ours, exceed $1 million.

As in many other industries, the large, well financed seemed to be better prepared than those who are less sophisticated and more personally operated. I would rate the dairy industry as possibly receiving a "C" for overall preparedness.

WHAT CAN CONGRESS DO TO HELP?

Many persons are not aware of the real potential for disaster that exists. This committee is an excellent vehicle toward a broader awareness level nationwide.

Some suggestions for Congress to act upon:

1. Establishing a centralized, government sponsored web page for all U.S. companies to log on to and certify they are completely compliant. Companies could access this page to verify if their suppliers and customers are prepared to function after January 1, 2000. This would reduce duplication of effort.
2. Immediate tax recovery of all program upgrade costs. I understand that the IRS has stated that the portion of any new software or hardware needed for Y2K compliance could be expensed in the current year. However, much of the software and hardware needed to operate the new upgrades will not be immediately deductible as an expense since it is not used solely for Y2K but may incidentally improve other non-Y2K functions of the operating systems. This upgrade must be expensed over a longer period of time under the current IRS guidelines.
3. Assure the industry that government services will be fully compliant. I understand many Federal, State, and local public bodies such as utilities, emergency services, financial institutions, and transportation services are not Y2K compliant and do not have the resources to become compliant by January 1, 2000.

I thank you for this opportunity to express the Y2K status of our cooperative in Oregon. Hopefully it can help others avoid a major crises just 65 weeks from now.

SUMMARY OF TILLAMOOK® CHEESE Y2K ISSUE

Upon our February 1996 audit, of our 1995 financial records, it became apparent that we should begin immediately to address the potential problems in our computer systems when January 1, 2000 occurs. TCCA selected staff to attend Lucent seminar to gain understanding of the diverse elements that will be affected by the Y2K issue (legal issues, banking and commerce, supplier compliance, and order processing).

Our MIS staff of two people took it upon themselves to form internal teams to research how the Y2K issue will effect the daily operations of our company in each department. These teams determined that none of our major systems (Accounting System, Patron Payroll System, EDI Software, Payroll software, other smaller applications, and our PBX Voice Mail system) were Y2K compliant. As a result, these teams evaluated and selected new applications to replace almost all major systems in the organization.

MIS is also in the process of determining the general preparedness of our contacts in the food manufacturing industry. We have received over 10 letters of certification and surveys assessing the level of the problem within this entity.

1. Research of the Y2K Crisis:

—Gain understanding of the impact the Y2K issue will have on our network infrastructure, computing hardware, and major software systems

—More specifically how will this effect plant operations (staff), customers, manufacturing industry, and budget

— Preparation of other companies

2. Compliance Requirements:

—Written high-level plan that outlines TCCA's procedures for Y2K issue (include cost estimate)

—Identify and schedule staff for plan implementation

—Timetable of expected completion dates

—Prepare comprehensive inventory of financial, informational and operational systems

—Identify critical systems and decide which are negatively impacted

—Plan for renovation, replacement and upgrade

—Contact key vendors, service providers, and customers to determine their systems compliance

—Mitigation of risk of litigation and non-compliance

—Contingency plan for systems failing to function properly

—Delegate MIS and administration to oversee Y2K issue

3. Year-To-Date Status

—Selected new Windows Accounting Application (Platinum for MS SQL) and implementation has begun—conversion process expected to last through 5/99

—EDI software upgraded to Sterling Gentran (also on MS SQL) and is ready for installation and implementation—completion of this process is pending on the interfacing Accounting system—expected to be in place by 12/98

—Payroll software (ADP for SQL) replaced and in use since 9/98

—Still searching for a new software application to replace Patron Payroll system—currently assessing Windows based system developed in New Zealand—expected implementation 6/99

—Currently upgrading PBX Phone and Voice Mail system

—On-going testing of all equipment and desktop applications for Y2K compliance

—Currently developing three phase implementation of HMI system (Wonderware Factory Suite) to control and monitor the production process for all products—scheduled completion Fall 1999 (note that we can still make cheese if computer shuts down)

—Currently assessing compliance of our suppliers, trading partners, business associates, etc. * * * and to inform them of our plans in progress

—Established estimated budget for implementation of plan:

Accounting	$450,000
Patron Payroll	100,000
EDVADP	25,000
Farm Store	40,000
Visitor's Center	100,000
Total cost	715,000

(Cost expected to be well over a million dollars, not including staff time)

RESPONSES OF HAROLD SCHILD TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. You mentioned that you first became aware of the Y2K problem during your company's February 1996 audit. Can you describe how exactly the problem came to the company's attention? What problems in your systems did you encounter which led you to believe there was a potential problem?

Answer. The management letter comment was first made as part of the 1996 audit, with the letter released in March 1997. This was becoming an automatic inquiry by auditors at the time to start looking at what their clients were setting up for Y2K. It was a comment to mean that we, along with other companies, should start addressing the Y2K problem. I would assume the Y2K issue was in almost everybody's management letter that year. It wasn't really that TCCA, or other companies were oblivious to the problem, but a comment directed to boards and management that it was an area that was going to have to be addressed.

Question 2. You mentioned that Tillamook has been unable to attract additional staff to cope with your programming demands. What impact will it have on your Y2K readiness if you can't obtain the needed assistance in the programming area? Do you have any suggestions about how to remedy this problem?

Answer. We are looking for an additional person right now. As we talked about, we need to get better organized, and take care of a lot of administrative matters, such as documentation, Y2K compliance progress, user training and procedures, etc. Without that, and if we can't get the right person, too much of what we do will be hit or miss, with whatever problem screams the loudest getting the most immediate attention. I think we probably can attract the right person, unless we run into the restraints of the overall company staffing budget which can be adjusted administratively. It is true that programmers are in high demand right now, and I would be scared if we weren't really putting in brand new software-farm store, Wonderware, Platinum, retail, etc. If we were trying to rewrite everything ourselves, I don't think we would ever get it done. I don't really know how to remedy the problem.

Question 3. What will the impact of Y2K costs be on your dairy members who are already struggling to keep their business viable?

Answer. First of all, the estimated costs to TCCA as a manufacturing and marketing cooperative are in the $1 million range for the fiscal years of 1998 and 1999. That amount will impact each of our 150 members by about $6,500 for the year. In a cooperative, all income that is not expended to cover operations is paid to members in either monthly payments for milk or year-end distribution of retained earnings.

There is no way yet to estimate how much it will cost to evaluate and correct the on-farm equipment such as automated milkers, feeders, environmental systems, herd record keeping, or computerized automotive controls. Each farm could experience different impacts depending on their level of electronic sophistication.

Question 4. You rated the dairy industry as a "C" for overall Y2K preparedness. What evidence can you cite to support conclusion? What specific steps do you recommend the dairy industry take to improve this rating?

Answer. The grade of "C" was given mostly on antidotal perception. Some fellow dairy executives readily discuss the level of effort they have expended on the Y2K problem. Most, however, are reluctant to discuss the issue or they openly state skepticism that the Y2K problem is real. The higher the level of retail involvement a dairy has, the more likely it is to be prepared for Y2K.

Question 5. One of your specific recommendations for the committee was that the Congress should establish a web page for all U.S. companies to log on to and certify that they were completely compliant. Assuming the U.S. Congress could accomplish this as a requirement for all U.S. businesses. If there were not major fines for submitting false data and certifications, what would be the inceptive for any firm to submit anything other than an affirmative that they were compliant? Would you believe the statements found at such a web site?

Answer. If a web site were established it should include legal penalties for false statements. The Commerce Department could research any complaint and rule on the liability for misrepresentation.

I would believe few companies would make false statements of compliance under the threat of legal action. In general, we do business with companies we know and have experienced good relations with. Those we do not know as well are now checked out through other companies' experience.

The system might not be perfect, especially if implemented in a short time frame. However, such a central clearing site would be preferable to not having any way to know if your partners in business are Y2K compliant.

Prepared Statement of Senator Gordon Smith

Thank you Mr. Chairman. I appreciate the opportunity to lead the effort in addressing the business sector on Y2K issues.

I would like to thank all the distinguished witnesses before us today for taking time to testify, and for helping us address the challenges facing the entire business sector at both the small and large ends of the scale. And with American businesses today becoming more and more dependent on technology, I hope this hearing will be a stepping stone for all small businesses to inch closer to full preparedness for the Year 2000.

Those most at risk from Y2K failures are small and medium-sized companies, not their larger counterparts. Many small companies have not yet realized the extent to which the Y2K computer problem will affect their businesses. And they may not have access to capital to cure such problems before the Y2K issue causes disastrous effects. This is why it is so important for the federal government to both raise awareness of the problem as well as the emerging solutions.

In my former life, before serving as a U.S. Senator, I was a pea picker from Pendleton, and owned a small frozen food processing plant. I can assure you that any interruption within the farm-to-fork chain can result in not only a direct loss to those who supply food, but will likely translate into food shortages and price increases nationwide. As with many businesses, food suppliers are increasingly dependent on computerized processing and information exchange.

For example, farmers and ranchers use electronically-equipped irrigation systems, animal systems and transport systems. Food processors rely on automated systems that help prepare and package consumer-ready products. Distributors, wholesalers, and retailers depend on computer-driven equipment to transport, deliver, store, display, and sell food products. Inventory and accounting systems, harvesting equipment, grain elevators, refrigeration and security systems also depend on the computations of computers.

Mr. Chairman, I am aware that in preparing for this hearing, our Committee has encountered some difficulties in securing witnesses from the major U.S. food retailers and manufacturers. I regret that these retailers and manufacturers cannot join us today. I would like to extend to them another invitation to join us next year as we continue to address the food industry and the important role they play in the world's food market.

However, I am happy to report that we will hear from a representative of one of Oregon's food companies, many of whom have been working very hard to assure that they are Y2K compliant.

I am proud to introduce Harold Schild, President and CEO of Tillamook County Creamery, who is one of our witnesses today from Tillamook, Oregon. I look forward to hearing Mr. Schild's testimony to address the "real" problems with which a typical small business is confronted and its approaches for addressing the Y2K problem.

Another company from Oregon, Norpac Foods, has also been leading the efforts in addressing the Y2K problem in the frozen food business. While Norpac's representative is not present today, the company has provided a statement to be entered into the record.

I am very pleased to see the Deputy Administrator of the Small Business Administration, Mr. Fred Hochberg, here before us today. The SBA has been one of the few leading federal agencies actively raising public awareness for Year 2000, and I would like to commend the agency for its aggressive outreach programs to small businesses. I know my constituents in Oregon have found the SBA web site very useful and informative.

Mr. Hochberg, I am interested in your opinion regarding the recent legislation, passed by the Senate Small Business Committee, that requires the SBA to establish a Y2K Loan Program. I understand this loan program would establish a new short-term loan program under which the SBA would guarantee up to 50 percent of the value of private-sector loans, up to a total loan value of $50,000 for small businesses to become Y2K-compliant. If you or any of the witnesses can testify on the impact this legislation will have on the small businesses of America, I would be very interested.

As we work toward addressing the Y2K problem, let's not forget that many of our international neighbors are still very far behind. We need to continue to encourage foreign countries to focus on the impacts of Y2K, since it could potentially shut down an entire country. With this in mind, I look forward to learning more about the specific Y2K challenges facing both our small businesses and global corporations.

Thank you Mr. Chairman.

PREPARED STATEMENT OF SENATOR OLYMPIA J. SNOWE

Mr. Chairman: Thank you very much for holding today's hearing regarding how the year 2000 computer problem will impact small businesses. When I wrote to you in August, encouraging you to hold this hearing, it was after I held a series of forums about this problem and how this problem impacts small businesses. I planned the forums in Maine because I felt that it was very important to bring the Year 2000 computer problem issue to the attention to small businesses.

I am very glad I did because I learned a lot about the problem. I learned that this is a very serious problem for small businesses. I learned that it will take a great deal of effort by the operators of the small businesses to correct this problem. I also learned, like most things today, a solution to this issue will require an investment of time and money and a concerted effort to ensure that small businesses are aware of the problem and are encouraged to solve it now, rather than later.

As Rod Rodrique of the Maine Manufacturing Extension Partnership will tell you during his testimony, the forums were an overwhelming success and people who attended learned a great deal about the problem, as I did. Mr. Chairman, I am happy to report that as a result of the forums, many small businesses in Maine are working to ensure that they are Year 2000 compatible. I hope they complete the work on time.

Today, as we all know, almost every aspect of our lives are influenced by computers. Everything from buying groceries, to phoning the office, to getting money from the ATM machine, all rely on the computer to process information needed to conduct these transactions. And certainly, just as small businesses form the backbone of our economy, computers have come to form the backbone of our small business operations.

I decided to convene these first-of-its kind in the nation forums throughout Maine this past August because the clock is literally ticking on our opportunity to fix the Y2K problem. As the last grains of sand slip through the 20th century hourglass, the clocks inside an estimated 200 million computers across America are counting down toward what could be a disaster for the country and private enterprises across the United States.

We've all heard the humorous twist on an old saying: "Why do today what you can put off until tomorrow?" Well, after December 31 of next year, there won't be a tomorrow for computers that, despite being able to balance multi-million dollar ledgers, won't even know what day it is. In other words, instead of New Years' being a time for celebration, it could be a time for consternation—and perhaps the greatest collective hangover this country's ever known.

In all seriousness, though, the impact on the small business community could be significant. According to a National Federation of Independent Business and Wells Fargo Bank study, 82 percent of small businesses are at risk.

Fortunately, it doesn't have to be that way. With the benefit of foresight and proper planning, we can diffuse this ticking time bomb and ensure that the business of the nation continues on without a hitch—or a glitch.

From a technical standpoint, the corrections are not difficult to make. However, determining that there's a problem, finding people qualified to fix the problem, and crafting a solution to fit the individual needs of different computers and programs poses significant challenges.

For one, to determine whether a system needs to be fixed, the software code must be reviewed, which often entails reading literally thousands or even millions of lines of computer code.

Furthermore, there is a serious shortage in this nation of workers skilled in performing this task—especially those who can decipher older computer languages which may no longer be taught in school, but are likely to contain the Y2K "bug".

Finally, there is no set method of curing the problem. A magic "one size fits all" solution simply does not exist, and it will be up to each individual technician to determine the proper course of action. That is why it is so important that we start now to fix the problem.

On the federal level, the Senate Commerce Committee, of which I am a member, has been working to address the situation, which poses the threat of having a serious negative impact on the U.S. economy over the next few years. In fact, a recent study by Standard Poor's determined that, due to the Year 2000 computer problem, economic growth could be cut by half a percentage point in 2000 and early 2001, a result that would be similar to the economic damage expected from the Asian financial crisis.

Major industry sectors must coordinate their efforts to correct their computer systems so they continue to function as designed. Especially among banks, credit unions, and the stock market, the perils of inaction could be millions of transactions lost, resulting in billions of dollars being transferred to wrong accounts, or accounts rendered inaccessible.

These are important reasons not to wait another day to tackle this issue, but as a member of both the Commerce and Small Business Committees, back in April when the Commerce Committee was having a hearing on this very topic, I began to wonder what the effects would be on small business as well. After discussing this issue with people in Maine, I discovered that, in fact, small businesses were aware of the issue but have not focused on the problem.

I know many small businesses simply don't have the kind of time and resources that many larger businesses may have at their disposal to fix this potentially serious problem. In order to provide small businesses assistance, I joined Senator Kit Bond as an original co-sponsor of legislation that will help small businesses solve their Y2K problems.

Under this legislation, the Administration will establish a pilot loan guarantee program under which it will provide loans up to $50,000 to small businesses to address the issue. I believe this is a critical way in which the federal government can help finance the purchase or repair of computer equipment to achieve Y2K compliance.

With that, I'd like to again thank you for holding this very important hearing.

PREPARED STATEMENT OF RONALD J. STRECK

INTRODUCTION

Good morning. My name is Ron Streck and I am President and CEO of the National Wholesale Druggists' Association (NWDA). NWDA appreciates the invitation to testify today before the committee about the implications of the Y2K "bug."

NWDA is the national trade association representing distributors of pharmaceutical and related healthcare products. NWDA active member companies operate 215 distribution centers throughout the country that service every state, the District of Columbia and U.S. territories. NWDA's active members provide distribution services to the 130,000 pharmacy outlets in the country, including the 21,000 independent pharmacies, 18,000 chain pharmacies, 7,500 hospital pharmacies, 220 mail order pharmacies, 7,000 food stores, 5,000 mass merchandisers, 4,000 long-term care and home health facilities, 56,000 clinics and 1,000 HMO's.

Our most recent data indicates NWDA-member wholesale distributors, on average, obtain products from over 750 manufacturer suppliers. Typically, a single wholesale distribution center stocks an average of 24,000 items and will process over 13,000 order lines per day. Virtually all orders placed by pharmacy customers to their wholesale distributors are transmitted electronically and more and more "electronic" picking devices are used to fill these orders.

To service an increasingly demanding and integrated healthcare market, practically all wholesalers provide daily deliveries with a growing number of wholesalers providing twice-a-day deliveries to their customers. However, today's wholesalers do so much more than "just" deliver product in a timely manner. Some of the value-added services NWDA members provide to their customers include marketing and advertising support, product sourcing programs and special handling services. Other services provided that are especially relevant to the Y2K discussion are the computer and information programs that include third party claims processing and receivables services, inventory management, pharmacy computer systems for dispensing and care, and point-of-sale systems.

Wholesalers have been innovators and leaders in information technology. They continue to use information technology to integrate suppliers and customers. These programs and systems rely on automation, connectivity, information systems, electronic linkages and network building that allow for the prompt and efficient delivery of life saving healthcare products. NWDA members have been methodically working to ensure their systems and those of their customers are compliant. You will hear more about exactly what wholesalers have been doing from Keith Mallonee of the McKesson Corporation in a few minutes.

Based on the number of suppliers, customers and orders, it does not take long to speculate on what would happen if there were an interruption of electronic transfer of information. Many of these transmissions are reliant on commercial and government telecommunication networks—systems over which the pharmaceutical industry has no control. NWDA and its members need to know that these vital communication networks are Y2K compliant and ready to support the delivery of healthcare services to the patient. This constant electronic transfer of information is the reason I am here today.

NWDA and our members have long been concerned with the potential for Y2K problems. This topic was first discussed in 1993 when the association began an initiative to raise awareness of the problem in the industry and develop a plan of action. In the subsequent years, NWDA's Technical Standards Committee, Productivity Committee, and Business Systems Committee have addressed the issue and it has been highlighted numerous times in the association's newsletter. NWDA staff have been active participants in the process that developed Y2K standards among EDI standards' groups and in the adoption of Year 2000 compliance standards required under the Health Insurance Portability and Accountability Act. In addition, NWDA's long-range strategic plan includes a specific goal to "set up a system to share information on solutions to the Y2K problem by 1998."

As we have developed our association's webpage, NWDA has devoted a separate section just for dissemination of general Y2K information. We endorse the notion of common solutions for common process problems and we are ready to move ahead with an industry clearinghouse for Y2K technical fixes that would allow drug wholesale trading partners to freely share such technical information. We have been reluctant to proceed with this project due to liability and antitrust concerns. However, with the passage of the Year 2000 Information and Readiness Disclosure Act (S. 2392) we understand that we will now be able to move ahead. We commend Congress for its approval of this important legislation and urge the President to move swiftly to sign the bill into law.

CONCERNS

We are greatly concerned that federal, state and local governments are quickly running out of time to adequately test and correct all public service and infrastructure systems. It is disturbing to read reports from Congress and the General Accounting Office indicating that there are serious concerns that many federal agencies will not be ready. The July 1998 report by the GAO entitled "Year 2000 Computing Crisis" concluded that "federal agencies and state governments suggest that the full extent of the managerial and operational challenges posed by the heavy reliance on others for data needed to sustain government activity is not yet known."

Congressman Steve Horn, in his role as chairman of the House Subcommittee on Government Management, Information and Technology, has issued another report card on federal agencies with HCFA once again receiving an "F." We fear that federal and state government agencies will not survive the change over to Year 2000 without interruptions in healthcare reimbursements. Let me explain the impact a failure in the Medicare/Medicaid programs could cause in the delivery of prescription drugs.

Wholesalers operate on very low profit margins (1997 figures show a net profit after taxes of 0.76 percent) and extend credit to their customers who also operate on very tight margins. Over 75 percent of prescription drugs are reimbursed through various third party and government programs. Pharmacies and hospitals purchase products on credit with the expectation that there will be a continual flow of reimbursement to offset these expenses. If prescription drug reimbursements for their Medicaid and Medicare patients should be interrupted for any length of time, we are concerned that many retail pharmacies and rural hospitals will not be able to weather the storm.

A related concern is the emerging role wholesalers have recently taken to manage their customer's receivables. Wholesalers, as part of their customer service program, will buy the receivables from their pharmacy customers and pay them within three days. Typically, the wholesaler must then wait 30 to 90 days to be reimbursed by the third party payer. If the government or other payers are not Y2K compliant, it will seriously imperil the cash flow for the wholesalers and their customers.

Government reimbursement is only one area that could disrupt the flow of life sustaining prescription drugs to patients. Even if all parts of the prescription drug supply chain are compliant and ready, if there are failures in other links, it would be irrelevant that we are ready. We need assurances that government agencies will be Y2K ready so they can seamlessly carry out their important functions. If they are not, and drug wholesalers therefore cannot provide pharmaceuticals to the pharmacy or hospital when they are needed, the results could be catastrophic. Additionally, failures within the transportation, communications, public utility or financial networks will have a great impact on our sector. All these systems are interconnected and disruption in one causes disruption throughout the entire system.

We are hearing that patients and providers are starting to talk about trying to stockpile products as a contingency plan. This is not a realistic approach and one that could prove to be very dangerous to the patient. Not only are there cost and efficiency concerns, but more importantly, there are safety and efficacy issues revolving around the integrity of the product due to expiration dates and sensitive storage requirements. In addition, if a DEA registrant suddenly increased its normal ordering pattern for controlled substances, a "suspicious order" report would be generated and investigation of these events would put an unnecessary and avoidable drain on law enforcement resources. Also, many patients are prohibited under their insurance plans from obtaining more than a 30-day supply of their prescription. Clearly, stockpiling or hoarding prescription drugs is not the answer.

CONCLUSION

Wholesalers are making contingency plans to make sure there is not a disruption in the availability of product. I want to emphasize that wholesalers are just one link in the chain. If the government agencies that play such a vital role in the health care system are not going to be Y2K compliant, contingency plans must be quickly completed and this information passed on to the public. How a business or industry develops its own backup plan depends on what government services will be available. NWDA and our member companies stand ready to work with government, at all levels, to address these issues to ensure that life saving medicines continue to get to those who need them when they need them. Time is of the essence. I thank the Committee for holding this hearing today to address this momentous issue.

RESPONSES OF RONALD J. STRECK TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question. Mr. Streck, even though your industry deals with 750 pharmacy suppliers and 130,000 outlets in the country, you rate government agencies as one of your top Y2K concerns. Will you please tell the Committee which government agency you are most concerned about and why?

Answer. Government agencies are not our only concern. For example, we are concerned about the Y2K readiness of our trading partners, pharmacy customers, utility companies and telecommunication networks. However, we continue to hear reports from the GAO and others that numerous government agencies are behind in their efforts to become Y2K compliant.

We are concerned that HCFA will not be ready. Indeed, in a September 1998 report, the GAO concluded that "Despite its actions to improve the direction and oversight of the Y2K effort, HCFA's Y2K progress is significantly behind schedule." HCFA concerns us because of the impact a disruption in the reimbursement schedule would have on pharmacy providers participating in the Medicare and Medicaid programs. It could be especially devastating for small retail pharmacies. The ripple effect on drug wholesalers could also be dramatic due to the emerging role they are taking in managing their customer's receivables. As discussed in my testimony, "Wholesalers, as part of their customer service program, will buy the receivables from their pharmacy customers and pay them within three days. Typically, the wholesaler must then wait 30 to 90 days to be reimbursed by the third party payer. If the government or other payers are not Y2K compliant, it will seriously imperil the cash flow for the wholesalers and their customers."

Another federal agency that has a significant impact on drug wholesalers is the Drug Enforcement Administration (DEA), due to its oversight responsibilities in tracking controlled substances. Drug wholesalers need reassurance that DEA's systems will be prepared to deal with the Y2K problem and that there will not be a disruption in the distribution of controlled substances. Because drug wholesalers receive and distribute products via the nation's highways, we are also concerned that the systems related to this are compliant. It is very disturbing to read in a GAO report (March 1998, GAO/T-AIMD–98–101) that "highway safety could be severely compromised because of potential Year 2000 problems in operational systems."

The readiness of state agencies that administer programs that complement or parallel federal programs are also of concern. For example, if HCFA were Y2K compliant but the state agency that administers the Medicaid program is not, there will be disruptions.

Finally, I want to clarify one of the numbers cited in the question—on average, a wholesaler will deal with 750 suppliers; overall, there are approximately 2,000 such suppliers in the country.

Question. Please explain to the Committee how the Drug Enforcement Agency (DEA) becomes involved if patients or providers stockpile drugs in anticipation of the Y2K problem?

Answer. The DEA is responsible for monitoring the distribution of controlled substances. As you know, these drugs are particularly susceptible to abuse and therefore the oversight is strict. For example, the DEA, through the U.S. Attorney General, sets an annual production quota for Schedule I drugs (high potential for abuse, no accepted medical use, used primarily in research settings) and Schedule II drugs (high potential for abuse, acceptable medical use with severe restrictions, abuse may lead to severe psychological or physical dependence). While stockpiling of Schedule I's is very unlikely, it could happen more readily with Schedule II drugs. Based on the quota amounts, which are established in the preceding year, orders by manufacturers for ingredient quantities are placed, production schedules are set, etc. well in advance of the time the product reaches the marketplace. If stockpiling does takes place toward the end of 1999, manufacturers will not be able to meet the needs of those patients who did not hoard and their lives will be in danger.

Under the supervision of DEA, there is also a highly regulated method for tracking controlled substances through the supply chain. When there is a significant change in ordering patterns or an unaccounted for variance, it is the obligation of the drug wholesaler to report this "suspicious order" to DEA. DEA then has the prerogative to investigate. It is our concern that if there were a marked change in ordering patterns in the final months of 1999, the DEA would have to expend significant resources to investigate.

I would like to reiterate that I do not believe that stockpiling is the answer. There are safety, efficacy, storage and waste issues that must be considered. As discussed in the next question, now is the time for health care providers and patients to be discussing alternatives to insure that necessary medications are available if Y2K problems result in a disruption of the regular supply channel.

Question. Does the wholesale drug industry have any plans to provide an emergency supply of drugs to people like Laurene West who will perish without them?

Answer. Virtually all drug wholesalers have contingency plans to deal with emergency situations. They have a history of providing life saving medications even when floods, earthquakes, hurricanes and other natural disasters have disrupted the normal flow of product. I am proud of the responsiveness and creativity of our industry in these situations. Ms. West should be commended for her proactive stance and recognized for raising important concerns. As always, drug wholesalers are ready to work with health care providers and their patients, who are especially dependent upon pharmaceuticals to maintain life, to have ready access to them. It is incumbent upon those providers and patients to be working together now to develop contingency plans should the Y2K "bug" alter the normal means of obtaining the necessary drugs.

Question. Would you please explain to the Committee your industry's plan for a web page for an industry clearinghouse for Y2K technical fixes?

Answer. NWDA established and maintains on our website a centralized page of links that provides industry-specific Y2K information. With the passage of the Year 2000 Information and Readiness Disclosure Act, we will be enhancing the site to include a list server and discussion forum for members to share appropriate Y2K information and solutions. It is my hope that we will be "up" in the next 30 to 45 days. Once it is operative, a major effort will be undertaken to publicize this resource to our membership.

Additionally, I am pleased to let the committee know that NWDA may be working with the Pharmaceutical Research and Manufacturers Association (PhRMA), the national association representing our country's pharmaceutical manufacturers, to facilitate dialogue between our respective members on this topic. We have just begun our discussions on this project and it may expand to include all segments of the pharmaceutical supply chain.

Question. Mr. Streck, you have stated that the constant transfer of information is the reason you are here today. Have you contacted the major telecommunication companies to tell them of your concerns and obtain reassurance that they will be operating on January 1, 2000?

Answer. The telecommunications sector touches virtually everyone in our country. It is my hope that Congress has sent a strong message to this industry that it is essential that it be Y2K ready on January 1, 2000.

Prepared Statement of Laurene L. West

Standing here before you this morning I probably appear to be in good health. I am not. Without daily medication and a coordinated effort from the health care community, I will be a casualty of the Year 2000—I will die.

I had a tumor removed from the center of my brain and now I require daily medication to prevent re-growth. Additionally, when I had the first of 13 surgeries on my head, I acquired a staph infection which does not respond to any known oral antibiotic. I am dependent on IV antibiotics which I can not stockpile as they expire in less than 30 days. A disruption to the supply of IV antibiotics will kill me.

I am a Registered Nurse—for more than 20 years I have worked in Critical Care areas of the hospital. Concurrently for the past 14 years, I have worked to develop and implement medical information systems. For the past two years I have worked with various health care organizations to help them prepare for the Year 2000 crisis.

I know health care. I know what impact the Year 2000 will have on healthcare.

My message today is two fold * * *

First—we have all read media reports expressing concern about potential power outages in the Year 2000 and the resulting effect on national security, financial institutions, air traffic control, etc. * * * all hospitals and health care facilities will be at significant risk without power. However, today, I want to suggest that a disruption in the medication supply will be more important than a disruption to the power supply. Nurses can keep patients alive with manual procedures—doing CPR for extended periods of time but we can not keep patients alive without medications.

The second message is that all Americans will be affected if there is a disruption in the supply and distribution of medications, particularly for those of us who are alive only because we have uninterrupted access to prescription medications.

Ladies and Gentlemen, my medications requirements are minimal compared to those of many other Americans. Millions of insulin dependent diabetics, cardiac patients, transplant patients (kidney, heart, lung, cornea—all organs) will die if their medication requirements are not met.

We need to begin immediately to teach the American public what they can do to prepare. We need a massive, national public awareness/education program so that we can minimize the number of Year 2000 related casualties. An informed and educated public will be less likely to panic * * * causing social unrest because prescription drugs are not available.

All medication dependent Americans are looking to you to help mobilize national resources to help us survive. I want to help with this process, all I need are funding and your influence.

Let's work with the RX2000 Solutions Institute, health care organizations represented in this room, the American Medical Association, AARP, The International Red Cross, as well as federal resources to develop plans for a coordinated national preparedness program so that the Year 2000 does not cause unacceptable risks.

We need legislation allowing for a one time exclusion for Medicare or health plans allowing patients to receive a 90 day supply of medications instead of a 30 day supply. We need creative processes for distributions of controlled substances and radioactive isotopes. (All health plans should volunteer this option.) Just in time inventory is a big problem

Pharmaceutical companies—should be pressuring AMA, AHA, ANA, DOI to allow for this exclusion * * * may loose 50–70 percent of their client base by Q1 2000).

We need to work with the CDC (Center for Disease Control) to prevent global epidemics from a lack of antibiotics or immunizations.

We should compose a National "Patient Advocacy Council" to monitor Y2K efforts within all health care organizations. This could be an attachment to the RX2000 Institute. (I would like to chair this committee.)

Health care organizations should be required to stockpile medications and supplies as well as disclose their Y2K compliance progress with their patient population.

And, if worst case scenarios do occur, and health care is rationed, the public needs to know what procedures and diagnoses will be treated.

Thus far, most health care organizations have taken the stance that their liability exposure can be limited by keeping "in check" their due diligence efforts. (This may be politically and legally correct but I do not consider this to be ethical.) If WE do not teach the public, who will? There is no harm if we over react, many may die if we do not act.

I am willing to do whatever I can to help save as many lives as possible—mine included. My story is not unique, there are millions of people who know there is a problem but they do not know where to turn for suggestions or help. Let's help them.

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

NORPAC FOODS, INC.,
Stayton, Or, October 5, 1998.

Hon. GORDON SMITH,
U.S. Senate,
Washington, DC.

DEAR SENATOR SMITH: It is a privilege to respond to your request for information about how NORPAC Foods, Inc., Oregon's largest fruit and vegetable processor, is addressing Year 2000 (Y2K) issues.

As a large food processor, we are addressing Y2K issues to meet two long-range goals and specific near-term business objectives.

First, our actions are guided by our commitment to maintain and improve the critical trust relationship we have with our consumers at every level of our distribution process. This includes our 240 owner-growers, more than 4,000 employees, countless suppliers, and the citizens in the communities throughout Oregon where our facilities are located. Our public holds us to a critical standard and we take that responsibility very seriously throughout every level of our organization.

We have placed Y2K compliance in this trust category because of the critical interdependence NORPAC has with so many people, and the scores of inside and outside company business functions that are served by our computer system. There is the continuous expectation that both the quality and access to information, and how we and others use it, must not be adversely affected.

Second, we are a highly regulated business operating in an industry that must continue to meet many stringent standards established by federal, state or local governments, or the specific operating agreements we have with our growers, suppliers or vendors.

Recognizing these two trust goals and our primary operational objective to ensure that the goods and services we provide will flow without interruption as we move into the next century, we established our formal Y2K Project in 1997. This multiphase process has been implemented throughout every level of our company, with the ongoing support of our board of directors.

While you will find a more specific description of our plan attached to my letter, here is a summary of our actions.

Our initial and primary operational focus has been on our own internal computer system. This system integrates the operation of our company across five geographically dispersed locations and through shared business relationships with many other businesses outside of NORPAC. We have brought our information systems department together with plant operations and engineering to look at both common and specific issues and solutions.

Earlier this year, we required that any new software systems, whether developed internally or purchased externally, be Y2K compliant. To raise expectations with our suppliers and external business partners about NORPAC's standards, we sent a letter and readiness survey to prompt them to take appropriate actions.

These actions have resulted in a detailed assessment of where we are, particularly with our progress on coding changes to our own systems. Before the end of this year, we will have completed all testing and verification to ensure that our software changes are Y2K compliant.

Operationally, we are working to identify, assess and develop responses to problems in outside-manufactured processing equipment. This effort has been challenging, as suppliers are presenting a declining level of information about whether this equipment has time-dated chips. Ultimately, this will impact our re-packing of stored fruits and vegetables into ready-to-market consumer products, and the transportation and tracking of them more than one year from now.

Despite the fact that we have made a significant investment in information about the Y2K issue, and developed and implemented a very thorough and comprehensive response, many uncertainties remain.

The issues are larger than what will happen from a data processing or operational standpoint when we enter the new millennium. For example, what will our unknown legal exposure be? Where will a company like NORPAC be, who has made a very thorough effort to meet this problem, who then finds itself exposed to presently undefined legal liabilities?

We would encourage Congress, under your leadership, to craft some appropriate "firewall" legislation to acknowledge and protect those organizations, like NORPAC, who have made significant efforts to ensure Y2K compliance.

Senator Smith, from your own knowledge of the food processing business, you know that all of us take these issues very seriously. Because we are a food processor, we may hold ourselves to a standard of public trust that is unique, but we are not asking for unique protection.

Rather, we would encourage you and the Congress to look for ways to clearly acknowledge Y2K compliance, and provide every American business with an assurance that their efforts have created a foundation for the future not a springboard for a decade of unanticipated litigation.

In the spirit of sharing information about this important issue and reaching solutions to common problems, please look to NORPAC Foods as a participant with Congress and other interested parties. If you, or your distinguished colleagues, have any questions, please call me.

Thank you for your continuing leadership.

Sincerely,

RICK JACSON,
President and CEO.

NORPAC FOODS, INC. ACTION SUMMARY

—What is the issue? (1)
—What is our OBJECTIVE? (2)
—How did we get started and what have we done? (3)
—Where are we now? (4)
—What areas are there where there might be exposure? (5)

(1) THE ISSUE

Simply stated, computers (where ever they are used) may have a problem functioning January 1, 2000, due to a defect in date identification. Given our exposure, we needed to identify where we use computers and then ensure that the date issue will not negatively impact our operations.

(2) OUR OBJECTIVE

NORPAC views Year 2000 compliance as a company-wide issue and has a serious commitment to ensure that goods and services we provide will flow without interruption as we move to the next century.

A major activity has been to ensure our computer systems will function without interruption. We have involved Plant Operations and specifically, our Engineering Department to review all of our processing capabilities for compliance with the year 2000 issue.

(3) HOW DID WE GET STARTED AND WHAT HAVE WE DONE?

NORPAC established a formal Year 2000 Project in 1997. Awareness of the Y2K problem was communicated to all areas of the company, as well as the Board of Directors. Since 1997, our Information Systems Department has required that any new systems, whether internally developed or acquired from software vendors, are Year 2000 compliant when delivered. In early 1998 NORPAC encouraged its suppliers to take appropriate action as well. In February 1998, a letter and survey was sent to all NORPAC suppliers and external business partners. The goal was to raise awareness of NORPAC's expectations with its suppliers, to determine their readiness with the Y2K issues and to gain their commitment that they will be Year 2000 compliant.

(4) ASSESSMENT (WHERE ARE WE NOW?)

INFORMATION SYSTEMS: At this point we have done an extensive assessment as to the Y2K impact on our computer system processes. This includes our software (in-house developed or purchased), our computer hardware (both company computers and personal computers), and our data communication capabilities (including

EDI standards). We are rapidly completing the “coding” changes to our computer systems to make them Y2K compliant. We are now entering a testing phase, where all software changes need to be tested and verified. This is a critical and fairly lengthy process. We want to complete this effort, if at all possible, by the end of this year.

OTHER AREAS: As a food processor we have extensive processing equipment in our plants. Much of this equipment uses micro processors and PLC’s (programmable logical controllers) to monitor and control the processing. Fortunately, for us there is very little date manipulation. We also have the advantage that most of the control processors have manual override capability. We have concluded that our exposure in this area is very limited, and we have not had to conduct any rigid verification and testing procedures.

(5) EXPOSURE/CONCERNS

There are areas where we simply do not know if we will have a problem. These areas lie outside our control (power, transportation, banking systems). However, these “gray” areas do require us to be attentive to any information about the potential problems that might negatively impact us. This will be an on-going process up until 01/01/2000.

The INTERNET continues to provide a wealth of this information. We expect that Federal and State government will continue to provide information as well. We have already met with our local city government and with the state’s Y2K Project Leader. Issues like electrical power availability are now being discussed. It appears that complete assessment of exposure in many of these areas is still underway. As new information presents itself, and this creates concern for us on our company’s ability to carry on our business operation, contingency plans will need to be made more formal. This is an area that can impact us all; the private citizen, business or government. It seems appropriate that an information sharing initiative be established (whether that be on the INTERNET, town hall meetings or other formats).

○